

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

JC971 U.S. PTO  
09/811459  
03/20/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2000年 5月30日

出願番号  
Application Number: 特願 2000-160001

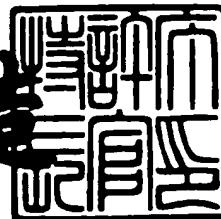
出願人  
Applicant (s): 株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 3月 2日

特許長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特 2001-3015403

【書類名】 特許願  
【整理番号】 H0000508  
【あて先】 特許庁長官殿  
【国際特許分類】 G09C 1/00  
【発明者】  
【住所又は居所】 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所 ソフトウェア事業部内  
【氏名】 桶屋 勝幸  
【特許出願人】  
【識別番号】 000005108  
【氏名又は名称】 株式会社日立製作所  
【代理人】  
【識別番号】 100096954  
【弁理士】  
【氏名又は名称】 矢島 保夫  
【手数料の表示】  
【予納台帳番号】 022781  
【納付金額】 21,000円  
【提出物件の目録】  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 楕円曲線暗号におけるスカラー倍計算方法及び装置、並びに記憶媒体

【特許請求の範囲】

【請求項1】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、前記判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行するステップとを含むことを特徴とするスカラー倍計算方法。

【請求項2】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、楕円曲線上の加算を実行した後、楕円曲線上の2倍算を実行するという順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項3】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、楕円曲線上の2倍算を実行した後、楕円曲線上の加算を実行するという順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項4】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を同時に実行するステップとを含むことを特徴とするスカラー

倍計算方法。

【請求項5】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

楕円曲線上の加算を実行するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の2倍算を実行するステップとを含むことを特徴とするスカラー倍計算方法。

【請求項6】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

楕円曲線上の加算及び楕円曲線上の2倍算の計算順序をランダム化するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、前記加算及び2倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項7】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算の計算順序をランダム化するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、前記加算及び2倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項8】

第1のデータから第2のデータを生成するデータ生成方法であって、請求項1から7の何れか1つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とするデータ生成方法。

【請求項9】

データから署名データを生成する署名生成方法であって、請求項1から7の何

れか1つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする署名生成方法。

【請求項10】

暗号化されたデータから復号化されたデータを生成する復号化方法であって、請求項1から7の何れか1つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする復号化方法。

【請求項11】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算装置であって、

前記スカラー値のビットの値を判定するビット値判定手段と、楕円曲線上の加算を実行する加算演算手段と、楕円曲線上の2倍算を実行する2倍算演算手段とを具備し、

前記ビット値判定手段により前記スカラー値のビットの値を判定した後、前記加算演算手段及び2倍算演算手段により楕円曲線上の加算及び楕円曲線上の2倍算を一定の回数及び一定の順序で実行し、スカラー倍点を計算することを特徴とするスカラー倍計算装置。

【請求項12】

請求項1から7の何れか1つに記載のスカラー倍計算方法に係るプログラムを格納したことを特徴とする記憶媒体。

【請求項13】

請求項1から7の何れか1つに記載のスカラー倍計算方法において、前記楕円曲線としてモンゴメリ型楕円曲線を用いることを特徴とするスカラー倍計算方法。

【請求項14】

請求項1から7の何れか1つに記載のスカラー倍計算方法において、前記楕円曲線として標数2の有限体上で定義された楕円曲線を用いることを特徴とするスカラー倍計算方法。

【発明の詳細な説明】

【0001】

## 【発明の属する技術分野】

本発明は、コンピュータネットワークにおけるセキュリティ技術に関し、特に楕円曲線暗号における暗号処理方法及び装置並びに記憶媒体に関する。

## 【0002】

## 【従来の技術】

楕円曲線暗号は、N.Koblitz, V.S.Millerにより提案された公開鍵暗号の一種である。公開鍵暗号には、公開鍵と呼ばれる一般に公開してよい情報と、秘密鍵と呼ばれる秘匿しなければならない秘密情報がある。与えられたメッセージの暗号化や署名の検証には公開鍵を用い、与えられたメッセージの復号化や署名の作成には秘密鍵を用いる。楕円曲線暗号における秘密鍵は、スカラー値が担っている。また、楕円曲線暗号の安全性は、楕円曲線上の離散対数問題の求解が困難であることに由来している。ここで楕円曲線上の離散対数問題とは、楕円曲線上のある点Pとそのスカラー倍の点dPが与えられたとき、スカラー値dを求める問題である。ここにおいて、楕円曲線上の点とは、楕円曲線の定義方程式をみたす数の組をいう。楕円曲線上の点全体には、無限遠点という仮想的な点を単位元とした演算、すなわち楕円曲線上の加法が定義されている。そして、同じ点同士の楕円曲線上の加法のことを、特に楕円曲線上の2倍算という。ある点に対し、特定の回数だけ加法を行なうことをスカラー倍といい、その結果をスカラー倍点、その回数のことをスカラー値という。

## 【0003】

楕円曲線上の離散対数問題の求解の困難性が理論的に確立されてきている一方で、実際の実装においては秘密鍵等の秘密情報に関する情報が暗号処理において漏洩する場合があり、その漏洩情報をもとに秘密情報を復元するといった、所謂パワーアナリシスという攻撃法が提案されている。

## 【0004】

DES(Data Encryption Standard)等の秘密情報を用いた暗号処理において、電圧変化を測定することで暗号処理経過を入手し、それをもとに秘密情報を推察するという攻撃法が、P.Kocher, J.Jaffe, B.Jun Differential Power Analysis, Advances in Cryptology: Proceedings of CRYPTO '99, LNCS 1666, Spring

er-Verlag, (1999) pp.388-397. に記載されている。この攻撃法は、DPA(Differential Power Analysis)と呼ばれている。

## 【0005】

楕円曲線暗号に対して上述の攻撃法を適用したものが、J.Coron, *Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.292-302.* に記載されている。楕円曲線暗号において、与えられたメッセージの暗号化や復号化、乃至は署名の作成及びその検証は、楕円曲線演算を用いて行なう必要がある。特に、楕円曲線上のスカラー倍の計算は、秘密情報であるスカラー値を用いた暗号処理において用いられる。

## 【0006】

また、モンゴメリ型楕円曲線  $Y^2 = X^3 + AX^2 + X$  ( $A, B \in \mathbb{F}_p$ ) を用いると標準型楕円曲線と呼ばれる通常用いる楕円曲線よりも高速に演算を実行できることが、P.L.Montgomery, *Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp. 48 (1987) pp.243-264.* に記載されている。これは、スカラー値の特定のビットの値に依存して、楕円曲線上の点の組  $(mP, (m+1)P)$  から点の組  $(2mP, (2m+1)P)$  乃至は点の組  $((2m+1)P, (2m+2)P)$  を繰り返し計算するスカラー倍計算方法において、モンゴメリ型楕円曲線を利用することにより、加算及び2倍算の計算時間が短縮されることに由来する。

## 【0007】

また、標数2の有限体上で定義された楕円曲線に対しても、モンゴメリ型楕円曲線におけるスカラー倍計算方法を適応させたスカラー倍計算方法並びにそれに用いる加算方法及び2倍算方法が、J.Lopez, R.Dahab, *Fast Multiplication on Elliptic Curves over GF(2<sup>m</sup>) without Precomputation, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.316-327.* に記載されている。このスカラー倍計算方法における加算及び2倍算の計算時間が短縮されることにより、標数2の有限体上で定義された楕円曲線における通常のスカラー倍計算方法と比べて、スカラー倍計算が

高速に実行できる。

【0008】

楕円曲線暗号に対するDPA攻撃の対処法の一つとして、ランダム化射影座標を用いる方法が、J.Coron, *Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.292-302.* に記載されている。これはスカラー倍計算において、特定の値が出現するか否かを観測し、そこからスカラー値を割り出す攻撃法に対して、ランダムな値を乗することにより、特定の値が出現することを予測できなくなる対処法である。

【0009】

【発明が解決しようとする課題】

上記従来技術の楕円曲線暗号は、DPA等のパワーアナリシスによる攻撃については考慮されていなかった。それゆえに、パワーアナリシスによる攻撃を和らげるためには、秘密情報を用いた暗号処理において、必要な計算以外に余分な計算を行なうなどして、暗号処理経過と秘密情報との依存関係を弱くしなければならなかった。そのため、暗号処理に必要な時間が増大し、ICカード等の計算速度の遅いコンピュータや、膨大な数の暗号処理をこなすサーバ等においては、暗号処理効率の低下が目立つ状態にあった。そのうえ、暗号処理経過と秘密情報との依存関係を完全に断ち切ることはできなかった。また、暗号処理効率を優先しようとすれば、パワーアナリシスによる攻撃を受け易く、秘密情報が漏洩する可能性があるという状態にあった。

【0010】

本発明の目的は、パワーアナリシス等により暗号処理経過が漏洩しても、秘密情報自体は漏洩せず、しかも高速に暗号処理を実行できる暗号処理方法及び装置並びに記憶媒体を提供すること、特に、秘密情報であるスカラー値から楕円曲線上のスカラー倍点を計算する計算経過からスカラー値の情報を引き出すことができないスカラー倍計算方法を提供することにある。

【0011】

【課題を解決するための手段】

上記目的を達成するため、本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、前記判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行するステップとを含むことを特徴とする。

#### 【0012】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、楕円曲線上の加算を実行した後、楕円曲線上の2倍算を実行するという順序で行なうステップとを含むことを特徴とする。

#### 【0013】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、楕円曲線上の2倍算を実行した後、楕円曲線上の加算を実行するという順序で行なうステップとを含むことを特徴とする。

#### 【0014】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を同時に実行するステップとを含むことを特徴とする。

#### 【0015】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、楕円曲線上の加算を実行するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の2倍算を実行するステップとを含むことを特徴とする。

#### 【0016】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカ

ラー倍点を計算するスカラー倍計算方法であって、楕円曲線上の加算及び楕円曲線上の2倍算の計算順序をランダム化するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、前記加算及び2倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とする。

## 【0017】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算の計算順序をランダム化するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、前記加算及び2倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とする。

## 【0018】

また本発明は、第1のデータから第2のデータを生成するデータ生成方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。さらに、データから署名データを生成する署名生成方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。さらに、暗号化されたデータから復号化されたデータを生成する復号化方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。

## 【0019】

さらに、本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算装置であって、前記スカラー値のビットの値を判定するビット値判定手段と、楕円曲線上の加算を実行する加算演算手段と、楕円曲線上の2倍算を実行する2倍算演算手段とを具備し、前記ビット値判定手段により前記スカラー値のビットの値を判定した後、前記加算演算手段及び2倍算演算手段により楕円曲線上の加算及び楕円曲線上の2倍算を一定の回数及び一定の順序で実行し、スカラー倍点を計算することを特徴とする。

## 【0020】

さらに、本発明は、上述のスカラー倍計算方法に係るプログラムを格納したことと特徴とする記憶媒体にある。前記橙円曲線としてモンゴメリ型橙円曲線を用いるとよい。前記橙円曲線として標数2の有限体上で定義された橙円曲線を用いるとよい。

#### 【0021】

##### 【発明の実施の形態】

以下、本発明の実施の形態を図面を用いて説明する。

#### 【0022】

図11は、本発明の実施の形態に係る暗号処理システムの構成図である。この暗号処理システム1101は、例えばICカード内に設けられ、暗号化（あるいは、復号化、署名の作成や検証）の際に、あるメッセージ（値）1105を入力すると所定の計算を行なってあるメッセージ（値）1106を出力する処理を行なう。暗号処理システム1101は、暗号処理部1102、スカラー倍計算部1103、及び秘密情報格納部1104を備えている。特に、本実施形態のスカラー倍計算部1103は、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないものであり、これにより暗号処理システム1101は、暗号処理経過が漏洩しても秘密情報は漏洩しないシステムになっている。

#### 【0023】

図16は、図11の暗号処理システムにおける処理の流れを示すフローチャートである。図17は、図11の暗号処理システムにおける処理の流れを示すシーケンス図である。

#### 【0024】

図16において、暗号処理システム1101は、以下のようにして、与えられたメッセージ1105から暗号処理を行なったメッセージ1106を出力する。まず、メッセージ1105を暗号処理システム1101に入力すると、暗号処理部1102がそれを受け取る（ステップ1601）。暗号処理部1102は、スカラー倍計算部1103に、入力メッセージ1105に応じた橙円曲線上の点を与える（ステップ1602）。スカラー倍計算部1103は、秘密情報格納部1104より秘密情報であるスカラー値を受け取る（ステップ1603）。スカラ

一倍計算部1103は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ1604）。スカラー倍計算部1103は、計算したスカラー倍点を暗号処理部1102に送る（ステップ1605）。暗号処理部1102は、スカラー倍計算部1103より受け取ったスカラー倍点をもとにして暗号処理を行なう（ステップ1606）。その結果を暗号処理を行なったメッセージ1106として出力する（ステップ1607）。

#### 【0025】

上記処理手順を図17のシーケンス図を用いて説明する。まず、暗号処理部1701（図11の1102）の実行する処理について説明する。暗号処理部1701は、入力メッセージを受け取る。暗号処理部1701は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部1702に楕円曲線上の点を与える。そしてスカラー倍計算部1702からスカラー倍点を受け取る。暗号処理部1701は、受け取ったスカラー倍点を用いて暗号処理を行ない、その結果を出力メッセージとして出力する。

#### 【0026】

次にスカラー倍計算部1702（図11の1103）の実行する処理について説明する。スカラー倍計算部1702は、暗号処理部1701より楕円曲線上の点を受け取る。スカラー倍計算部1702は、秘密情報格納部1703よりスカラー値を受け取る。スカラー倍計算部1702は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、暗号処理部1701にスカラー倍点を送る。

#### 【0027】

最後に秘密情報格納部1703（図11の1104）の実行する処理について説明する。秘密情報格納部1703は、スカラー倍計算部1702がスカラー倍を計算できるように、スカラー値をスカラー倍計算部1702に送る。

#### 【0028】

スカラー倍計算部1103が実行するスカラー倍計算は、スカラー倍計算経過

が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため、暗号処理部1102において、暗号処理を行なう際に暗号処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部1103のみであり、秘密情報に関する情報は漏洩しない。

#### 【0029】

次に、暗号処理システム1101におけるスカラー倍計算部1103の具体的な実施例を説明する。

#### 【0030】

図2は、暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第1実施例を示す図である。図1は、第1実施例のスカラー倍計算方法を示すフローチャートである。図1及び図2を参照して、第1実施例を説明する。

#### 【0031】

スカラー倍計算装置201では、点及びスカラー値207を入力し、以下の手順でスカラー倍208を出力する。ここで入力された点をP、入力されたスカラー値をd、出力するスカラー倍の点をdPで、それぞれ表すことにする。

#### 【0032】

ステップ101として、繰り返し判定部206において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ102として、2倍算演算部204により、点Pの2倍点2Pを計算する。ステップ103として、スカラー倍計算装置201に入力された点Pとステップ102で求めた点2Pを、点格納部202に点の組(P, 2P)として格納する。ステップ104として、繰り返し判定部206により、変数Iとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ113へ行く。一致しなければステップ105へ行く。ステップ105として、変数Iを1増加させる。ステップ106として、ビット値判定部205により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ107へ行く。そのビットの値が1であればステップ110へ行く。

#### 【0033】

ステップ107として、加算演算部203により、点格納部202に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ108へ行く。ステップ108として、2倍算演算部204により、点格納部202に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ109へ行く。ステップ109として、ステップ108で求めた点 $2mP$ とステップ107で求めた点 $(2m+1)P$ を点格納部202に点の組 $(2mP, (2m+1)P)$ として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ104へ戻る。

#### 【0034】

ステップ110として、加算演算部203により、点格納部202に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ111へ行く。ステップ111として、2倍算演算部204により、点格納部202に格納されている点の組( $mP, (m+1)P$ )から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ112へ行く。ステップ112として、ステップ110で求めた点 $(2m+1)P$ とステップ111で求めた点 $(2m+2)P$ を点格納部202に点の組 $((2m+1)P, (2m+2)P)$ として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ104へ戻る。

#### 【0035】

ステップ113として、点格納部202に格納されている点の組( $mP, (m+1)P$ )から、点 $mP$ をスカラー倍208として出力し、終了する。

#### 【0036】

以上の手順により出力する値である点 $mP$ が点 $P$ のスカラー値 $d$ によるスカラ倍の点 $dP$ となることは、計算過程において格納されている点の組( $mP, (m+1)P$ )の点 $mP$ に対するスカラー値 $m$ が、スカラー値 $d$ における先頭 $I$ ビットのビット列と一致することと、ステップ104においてステップ113へ行くと判定されるためには、 $I$ とスカラー値 $d$ のビット長が等しいことが必要である。

り、そのためスカラー値mとスカラー値dが一致することにより示される。

【0037】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。計算経過からスカラー値に関する情報を得る為には、少なくとも、各々のスカラー値に対する計算経過の間に違いが存在しなければならない。まず、あるスカラー値と、そのスカラー値との間に特定のビットのみが異なるスカラー値とについて考える。特定ビットが異なるので、計算経過において特定の回数だけ繰り返した後のステップ106でのビット値の判定の後、ステップ107へ行くかステップ110へ行くかの違いが生じる。しかしながら、ステップ107へ行ってもステップ110へ行っても、共にその後で加算を行ない、次に2倍算を行ない、そしてその結果を点の組として格納するという手順をとり、ステップ104へと戻る為、計算経過としての差異は存在しない。したがって同一の計算経過をとるためスカラー値の情報は引き出すことはできない。

【0038】

次に固定したビット長のスカラー値について考える。二つのビット長の同じスカラー値はいくつかのビットの値が異なる。値の異なるビットの数をkとし、与えられた2つのスカラー値をそれぞれd<sub>0</sub>及びd<sub>k</sub>とする。スカラー値d<sub>0</sub>とスカラー値d<sub>k</sub>の間でビットの値が異なる最初のビットに対して、その値がd<sub>k</sub>の対応するビットの値と等しく、その他のビットの値がd<sub>0</sub>の対応するビットの値と等しいようなスカラー値をd<sub>1</sub>とする。スカラー値d<sub>0</sub>とスカラー値d<sub>1</sub>は1ビットのみ値が異なる。次にスカラー値d<sub>1</sub>とスカラー値d<sub>k</sub>の間でビットの値が異なる最初のビットに対して、その値がd<sub>k</sub>の対応するビットの値と等しく、その他のビットの値がd<sub>1</sub>の対応するビットの値と等しいようなスカラー値をd<sub>2</sub>とする。スカラー値d<sub>1</sub>とスカラー値d<sub>2</sub>は1ビットのみ値が異なる。以下同様にしてスカラー値d<sub>k-1</sub>まで定める。スカラー値d<sub>0</sub>とスカラー値d<sub>k</sub>はkビットの値が異なるので、スカラー値d<sub>k-1</sub>とスカラー値d<sub>k</sub>は1ビットのみ値が異なる。したがって下付き指数の値が1だけ異なるスカラー値同士は1ビットのみ値が異なる。上述したように、1ビットのみ値の異なるスカラー値同士に

おいてはそれらの計算経過は同一となる。スカラー値  $d_0$  からスカラー値  $d_k$  まで 1 ビットのみ値の異なるスカラー値の連鎖が存在するので、スカラー値  $d_0$  とスカラー値  $d_k$  の計算経過は同一となる。ゆえに計算経過によりスカラー値の情報を引き出すことはできない。

## 【0039】

また、橢円曲線としてモンゴメリ型橢円曲線を用いると、加算及び 2 倍算が高速に実行可能であり、通常用いる標準型橢円曲線よりも高速にスカラー倍計算が実行可能である。

## 【0040】

標数 2 の有限体上で定義された橢円曲線に対しても、高速な加算及び 2 倍算の計算方法が知られており、上記手順において加算及び 2 倍算の計算にその計算方法を用いることにより、標数 2 の有限体上で定義された橢円曲線の通常のスカラーベ倍計算と比べて、高速にスカラーベ倍計算が実行可能である。

## 【0041】

図 5 は、図 11 の暗号処理システム 1101 における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラーベ倍計算方法の第 2 実施例を示す図である。図 4 は、第 2 実施例のスカラーベ倍計算方法を示すフローチャートである。図 4 及び図 5 を参照して、第 2 実施例を説明する。

## 【0042】

スカラーベ倍計算装置 501 では、点及びスカラー値 507 を入力し、以下の手順でスカラーベ倍 508 を出力する。ステップ 401 として、繰り返し判定部 506 において繰り返すか否かの判定を行なう為に、初期値として変数 I に 1 を代入する。ステップ 402 として、2 倍算演算部 504 により、点 P の 2 倍点 2P を計算する。ステップ 403 として、スカラーベ倍計算装置 501 に入力された点 P とステップ 402 で求めた点 2P を、点格納部 502 に点の組 (P, 2P) として格納する。ステップ 404 として、繰り返し判定部 506 により、変数 I とスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ 413 へ行く。一致しなければステップ 405 へ行く。ステップ 405 として、変数 I を 1 増加させる。ステップ 406 として、ビット値判定部 505 により、スカラ

一値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 407 へ行く。そのビットの値が 1 であればステップ 410 へ行く。

#### 【0043】

ステップ 407 として、2 倍算演算部 504 により、点格納部 502 に格納されている点の組 ( $mP, (m+1)P$ ) から点  $mP$  の 2 倍算  $2(mP)$  を行ない、点  $2mP$  を計算する。その後ステップ 408 へ行く。ステップ 408 として、加算演算部 503 により、点格納部 502 に格納されている点の組 ( $mP, (m+1)P$ ) から点  $mP$  と点  $(m+1)P$  の加算  $mP + (m+1)P$  を行ない、点  $(2m+1)P$  を計算する。その後ステップ 409 へ行く。ステップ 409 として、ステップ 407 で求めた点  $2mP$  とステップ 408 で求めた点  $(2m+1)P$  を点格納部 502 に点の組  $(2mP, (2m+1)P)$  として、点の組 ( $mP, (m+1)P$ ) の代わりに格納する。その後ステップ 404 へ戻る。

#### 【0044】

ステップ 410 として、2 倍算演算部 504 により、点格納部 502 に格納されている点の組 ( $mP, (m+1)P$ ) から点  $(m+1)P$  の 2 倍算  $2((m+1)P)$  を行ない、点  $(2m+2)P$  を計算する。その後ステップ 411 へ行く。ステップ 411 として、加算演算部 503 により、点格納部 502 に格納されている点の組 ( $mP, (m+1)P$ ) から点  $mP$  と点  $(m+1)P$  の加算  $mP + (m+1)P$  を行ない、点  $(2m+1)P$  を計算する。その後ステップ 412 へ行く。ステップ 412 として、ステップ 411 で求めた点  $(2m+1)P$  とステップ 410 で求めた点  $(2m+2)P$  を点格納部 502 に点の組  $((2m+1)P, (2m+2)P)$  として、点の組 ( $mP, (m+1)P$ ) の代わりに格納する。その後ステップ 404 へ戻る。

#### 【0045】

ステップ 413 として、点格納部 502 に格納されている点の組 ( $mP, (m+1)P$ ) から、点  $mP$  をスカラー倍 508 として出力し、終了する。

#### 【0046】

以上の手順により出力する値である点  $mP$  が点  $P$  のスカラー値  $d$  によるスカラ

一倍の点  $dP$  となることは、第1実施例の場合と同様に示すことができる。

【0047】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ406でのビット値の判定の後、ステップ407へ行くかステップ410へ行くかの違いが生じる。しかしながらステップ407へ行ってもステップ410へ行っても、共にその後で2倍算を行ない、次に加算を行ない、そしてその結果を点の組として格納するという手順をとり、ステップ404へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【0048】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

【0049】

標数2の有限体上で定義された楕円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

【0050】

図7は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第3実施例を示す図である。図6は、第3実施例のスカラー倍計算方法を示すフローチャートである。図6及び図7を参照して、第3実施例を説明する。

【0051】

スカラー倍計算装置701では、点及びスカラー値707を入力し、以下の手順でスカラー倍708を出力する。ステップ601として、繰り返し判定部706において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ602として、2倍算演算部704により、点Pの2倍点2Pを計算する。ステップ603として、スカラー倍計算装置701に入力された点Pとステップ602で求めた点2Pを、点格納部702に点の組(P, 2P)として格納する。ステップ604として、繰り返し判定部706により、変数Iとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ613へ行く。一致しなければステップ605へ行く。ステップ605として、変数Iを1増加させる。ステップ606として、ビット値判定部705により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ607へ行く。そのビットの値が1であればステップ610へ行く。

#### 【0052】

ステップ607として、加算及び2倍算演算部703により、点格納部702に格納されている点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP + (m+1)P及び点mPの2倍算2(mP)を同時に行ない、点(2m+1)P及び点2mPを計算する。その後ステップ609へ行く。ステップ609として、ステップ607で求めた点2mPと点(2m+1)Pを点格納部702に点の組(2mP, (2m+1)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ604へ戻る。

#### 【0053】

ステップ610として、加算及び2倍算演算部703により、点格納部702に格納されている点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP + (m+1)P及び点(m+1)Pの2倍算2((m+1)P)を同時に行ない、点(2m+1)P及び点(2m+2)Pを計算する。その後ステップ612へ行く。ステップ612として、ステップ610で求めた点(2m+1)Pと点(2m+2)Pを点格納部702に点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステ

ップ604へ戻る。

【0054】

ステップ613として、点格納部702に格納されている点の組（ $mP$ ,  $(m+1)P$ ）から、点 $mP$ をスカラー倍708として出力し、終了する。

【0055】

以上の手順により出力する値である点 $mP$ が点 $P$ のスカラー値 $d$ によるスカラ倍の点 $dP$ となることは、第1実施例の場合と同様に示すことができる。

【0056】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ606でのビット値の判定の後、ステップ607へ行くかステップ610へ行くかの違いが生じる。しかしながらステップ607へ行ってもステップ610へ行っても、共にその後で加算及び2倍算を同時にしない、そしてそれらの結果を点の組として格納するという手順をとり、ステップ604へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【0057】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

【0058】

標数2の有限体上で定義された楕円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

## 【0059】

図9は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第4実施例を示す図である。図8は、第4実施例のスカラー倍計算方法を示すフローチャートである。図8及び図9を参照して、第4実施例を説明する。

## 【0060】

スカラー倍計算装置901では、点及びスカラー値907を入力し、以下の手順でスカラー倍908を出力する。ステップ801として、繰り返し判定部906において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ802として、2倍算演算部904により、点Pの2倍点2Pを計算する。ステップ803として、スカラー倍計算装置901に入力された点Pとステップ802で求めた点2Pを、点格納部902に点の組(P, 2P)として格納する。ステップ804として、繰り返し判定部906により、変数Iとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ813へ行く。一致しなければステップ805へ行く。ステップ805として、変数Iを1だけ増加させる。ステップ806として、加算演算部903により、点格納部902に格納されている点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP + (m+1)Pを行ない、点(2m+1)Pを計算する。ステップ807として、ビット値判定部905により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ808へ行く。そのビットの値が1であればステップ811へ行く。

## 【0061】

ステップ808として、2倍算演算部904により、点格納部902に格納されている点の組(mP, (m+1)P)から点mPの2倍算2(mP)を行ない、点2mPを計算する。その後ステップ809へ行く。ステップ809として、ステップ808で求めた点2mPとステップ806で求めた点(2m+1)Pを点格納部902に点の組(2mP, (2m+1)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ804へ戻る。ステップ811として、2倍算演算部904により、点格納部902に格納されている点の組

( $mP$ , ( $m+1$ )  $P$ ) から点 ( $m+1$ )  $P$  の 2 倍算 2 (( $m+1$ )  $P$ ) を行ない、点 ( $2m+2$ )  $P$  を計算する。その後ステップ 812 へ行く。ステップ 812 として、ステップ 806 で求めた点 ( $2m+1$ )  $P$  とステップ 811 で求めた点 ( $2m+2$ )  $P$  を点格納部 902 に点の組 (( $2m+1$ )  $P$ , ( $2m+2$ )  $P$ ) として、点の組 ( $mP$ , ( $m+1$ )  $P$ ) の代わりに格納する。その後ステップ 804 へ戻る。

#### 【0062】

ステップ 813 として、点格納部 902 に格納されている点の組 ( $mP$ , ( $m+1$ )  $P$ ) から、点  $mP$  をスカラー倍 908 として出力し、終了する。

#### 【0063】

以上の手順により出力する値である点  $mP$  が点  $P$  のスカラー値  $d$  によるスカラー倍の点  $dP$  となることは、第 1 実施例の場合と同様に示すことができる。

#### 【0064】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ 807 でのビット値の判定の後、ステップ 808 へ行くかステップ 811 へ行くかの違いが生じる。しかしながらステップ 808 へ行ってもステップ 811 へ行っても、共にその後で 2 倍算を行ない、そしてその結果を加算の結果とともに点の組として格納するという手順をとり、ステップ 804 へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

#### 【0065】

また、橢円曲線としてモンゴメリ型橢円曲線を用いると、標準型橢円曲線よりも高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

## 【0066】

標数2の有限体上で定義された楕円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

## 【0067】

図15は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第5実施例を示す図である。図12、図13及び図14は、第5実施例のスカラー倍計算方法を示すフローチャートである。図12～図15を参照して、第5実施例を説明する。

## 【0068】

スカラー倍計算装置1501では、点及びスカラー値1507を入力し、以下の手順でスカラー倍1508を出力する。ステップ1201として、繰り返し判定部1506において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ1202として、2倍算演算部1504により、点Pの2倍点2Pを計算する。ステップ1203として、スカラー倍計算装置1501に入力された点Pとステップ1202で求めた点2Pを、点格納部1502に点の組(P, 2P)として格納する。ステップ1204として、繰り返し判定部1506により、変数Iとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ1213へ行く。一致しなければステップ1205へ行く。ステップ1205として、変数Iを1増加させる。ステップ1206として、演算ランダム化部1509により、加算及び2倍算の計算順序をランダム化する。加算、2倍算の順序で計算を実行する場合はステップ1301へ行く。2倍算、加算の順序で計算を実行する場合はステップ1401へ行く。

## 【0069】

ステップ1301として、ビット値判定部1505により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ1302へ行く。そのビットの値が1であればステップ1305へ行

の計算順序をランダム化する。加算、2倍算の順序で計算を実行する場合はステップ2405へ行く。2倍算、加算の順序で計算を実行する場合はステップ2402へ行く。

#### 【0087】

ステップ2402として、2倍算演算部2504により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ2403へ行く。ステップ2403として、加算演算部2503により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2404へ行く。

#### 【0088】

ステップ2405として、加算演算部2503により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2406へ行く。ステップ2406として、2倍算演算部2504により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ2404へ行く。

#### 【0089】

ステップ2404として、ステップ2402乃至はステップ2406で求めた点 $2mP$ とステップ2403乃至はステップ2405で求めた点 $(2m+1)P$ を点格納部2502に点の組( $2mP, (2m+1)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ2204へ戻る。

#### 【0090】

ステップ2213として、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から、点 $mP$ をスカラー倍2508として出力し、終了する。

#### 【0091】

以上の手順により出力する値である点 $mP$ が点 $P$ のスカラー値 $d$ によるスカラ一倍の点 $dP$ となることは、第1実施例の場合と同様に示すことができる。

#### 【0092】

また、橢円曲線としてモンゴメリ型橢円曲線を用いると、加算及び2倍算が高速に実行可能であり、通常用いる標準型橢円曲線よりも高速にスカラー倍計算が実行可能である。

#### 【0093】

標数2の有限体上で定義された橢円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された橢円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

#### 【0094】

図27は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第7実施例を示す図である。図26は、第7実施例のスカラー倍計算方法を示すフローチャートである。図26及び図27を参照して、第7実施例を説明する。

#### 【0095】

スカラー倍計算装置2701では、点及びスカラー値2707を入力し、以下の手順でスカラー倍2708を出力する。ステップ2601として、繰り返し判定部2706において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ2614として、ランダム化射影座標変換部2709により、乱数kを生成する。ステップ2615として、ランダム化射影座標変換部2709により、ステップ2614で生成したkを用いて、点Pを射影座標において、 $P = (kx, ky, k)$ と表す。ここで点Pは、アフィン座標では、 $P = (x, y)$ と表されるとする。ステップ2602として、2倍算演算部2704により、ステップ2615で $(kx, ky, k)$ と表された点Pの2倍点2Pを計算する。ステップ2603として、スカラー倍計算装置2701に入力され、ステップ2615で $(kx, ky, k)$ と表された点Pと、ステップ2602で求めた点2Pを、点格納部2702に点の組 $(P, 2P)$ として格納する。

#### 【0096】

ステップ2604として、繰り返し判定部2706により、変数Iとスカラー

値のビット長とが一致するかどうかを判定し、一致すればステップ2613へ行く。一致しなければステップ2605へ行く。ステップ2605として、変数Iを1増加させる。ステップ2606として、ビット値判定部2705により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ2607へ行く。そのビットの値が1であればステップ2610へ行く。

## 【0097】

ステップ2607として、加算演算部2703により、点格納部2702に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2608へ行く。ステップ2608として、2倍算演算部2704により、点格納部2702に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ2609へ行く。ステップ2609として、ステップ2608で求めた点 $2mP$ とステップ2607で求めた点 $(2m+1)P$ を点格納部2702に点の組( $2mP, (2m+1)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ2604へ戻る。

## 【0098】

ステップ2610として、加算演算部2703により、点格納部2702に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2611へ行く。ステップ2611として、2倍算演算部2704により、点格納部2702に格納されている点の組( $mP, (m+1)P$ )から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ2612へ行く。ステップ2612として、ステップ2610で求めた点 $(2m+1)P$ とステップ2611で求めた点 $(2m+2)P$ を点格納部2702に点の組( $(2m+1)P, (2m+2)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ2604へ戻る。

## 【0099】

ステップ2613として、点格納部2702に格納されている点の組（ $mP$ ,  
( $m+1$ ) $P$ ）から、点 $mP$ をスカラー倍2708として出力し、終了する。

【0100】

以上の手順により出力する値である点 $mP$ が点 $P$ のスカラー値 $d$ によるスカラ  
ー倍の点 $dP$ となることは、第1実施例の場合と同様に示すことができる。

【0101】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラ  
ー値に関する情報が漏洩しないことの根拠は、第1実施例における根拠と同様  
である。そのうえ、スカラー倍計算において、特定の値が出現するか否かを観測  
し、そこからスカラー値を割り出す攻撃法に対しても、最初にランダムな値を乗  
じている為、特定の値の出現を予測できなくなるので、そのような攻撃法に対し  
ても、スカラー値に関する情報が漏洩しないことがわかる。

【0102】

また、橙円曲線としてモンゴメリ型橙円曲線を用いると、標準型橙円曲線より  
も高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

【0103】

標数2の有限体上で定義された橙円曲線に対しても、上記手順において加算及  
び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2  
の有限体上で定義された橙円曲線の通常のスカラー倍計算と比べて、高速にスカラ  
ー倍計算が実行可能であることも、第1実施例と同様である。

【0104】

図28は、図27のランダム化射影座標変換部2709として使用するランダ  
ム化射影座標変換装置の一実施例を示す図である。図29は、このランダム化射  
影座標変換装置におけるランダム化射影座標変換方法を示すフローチャートであ  
る。

【0105】

ランダム化射影座標変換装置2801では、橙円曲線上の点2805を入力し  
、以下の手順でランダム化射影座標で表された点2806を出力する。ステップ  
2901として、座標判定部2802により、与えられた橙円曲線上の点280

5がアフィン座標で表されているか、それとも射影座標で表されているかを判定する。アフィン座標で表されていればステップ2902へ行く。射影座標で表されていればステップ2903へ行く。ステップ2902として、次のようにしてアフィン座標で表された点を射影座標で表す。アフィン座標で表された点を(x, y)とすると、射影座標として(x, y, 1)と表す。

## 【0106】

ステップ2903として、乱数生成部2803により、乱数kを生成する。ステップ2904として、射影座標変換部2804により、次のようにして射影座標で表された与えられた点をランダム化射影座標により表す。与えられた点を(x, y, z)とすると、乱数生成部2803で生成された乱数kを、各座標に乘じ、(kx, ky, kz)と表し、ランダム化射影座標で表された点2806として出力する。

## 【0107】

射影座標においては、0以外の任意の数kにより各座標を乗じても、同じ点と見做す。すなわち、(x, y, z)と(kx, ky, kz)は同じ点を表している。

## 【0108】

また、メモリ等の節約の為、ステップ2902の(x, y, 1)は実際に格納しなくとも、仮想的に(x, y, 1)と表されていると考え、ステップ2904で(kx, ky, kz)と表す際に、実際に格納を行なってもよい。

## 【0109】

図3は、図11の本実施形態の暗号処理システムを署名作成装置として利用する場合の構成を示す。図11における暗号処理部1102は、図3の署名作成装置301では署名部302になる。図18は、図3の署名作成装置における処理の流れを示すフローチャートである。図19は、図3の署名作成装置における処理の流れを示すシーケンス図である。

## 【0110】

図18において、署名作成装置301は、以下のようにして、与えられたメッセージ305から署名が付随しているメッセージ306を出力する。メッセージ

305を署名作成装置301に入力すると、署名部302がそれを受け取る（ステップ1801）。署名部302は、スカラー倍計算部303に、入力メッセージ305に応じた楕円曲線上の点を与える（ステップ1802）。スカラー倍計算部303は、秘密情報格納部304より秘密情報であるスカラー値を受け取る（ステップ1803）。スカラー倍計算部303は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ1804）。スカラー倍計算部303は、計算したスカラー倍点を署名部302に送る（ステップ1805）。署名部302は、スカラー倍計算部303より受け取ったスカラー倍点をもとに署名作成処理を行なう（ステップ1806）。その結果を署名が付随したメッセージ306として出力する（ステップ1807）。

#### 【0111】

上記処理手順を図19のシーケンス図を用いて説明する。まず、署名部1901（図3の302）の実行する処理について説明する。署名部1901は、入力メッセージを受け取る。署名部1901は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部1902に楕円曲線上の点を与え、そしてスカラー倍計算部1902からスカラー倍点を受け取る。署名部1901は、受け取ったスカラー倍点を用いて署名作成処理を行ない、その結果を出力メッセージとして出力する。

#### 【0112】

次にスカラー倍計算部1902（図3の303）の実行する処理について説明する。スカラー倍計算部1902は、署名部1901より楕円曲線上の点を受け取る。スカラー倍計算部1902は、秘密情報格納部1903よりスカラー値を受け取る。スカラー倍計算部1903は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、署名部1901にスカラー倍点を送る。

#### 【0113】

最後に秘密情報格納部1903（図3の304）の実行する処理について説明する。秘密情報格納部1903は、スカラー倍計算部1902がスカラー倍を計

算できるように、スカラー値をスカラー倍計算部1902に送る。

【0114】

スカラー倍計算部303が実行するスカラー倍計算は、上述した第1～第7実施例で説明したものがそのまま適用される。したがって、このスカラー倍計算は、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため署名部302において、署名作成処理を行なう際に署名作成処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部303のみであり、秘密情報に関する情報は漏洩しない。

【0115】

図10は、図11の本実施形態の暗号処理システムを復号化装置として利用する場合の構成を示す。図11における暗号処理部1102は、図10の復号化装置1001では復号部1002になる。図20は、図10の復号化装置における処理の流れを示すフローチャートである。図21は、図10の復号化装置における処理の流れを示すシーケンス図である。

【0116】

図20において、復号化装置1001は、以下のようにして、与えられたメッセージ1005から復号化されたメッセージ1006を出力する。メッセージ1005を復号化装置1001に入力すると、復号部1002がそれを受け取る（ステップ2001）。復号部1002は、スカラー倍計算部1003に、入力メッセージ1005に応じた橍円曲線上の点を与える（ステップ2002）。スカラー倍計算部1003は、秘密情報格納部1004より秘密情報であるスカラー値を受け取る（2003）。スカラー倍計算部1003は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ2004）。スカラー倍計算部1003は、計算したスカラー倍点を復号部1002に送る（ステップ2005）。復号部1002は、スカラー倍計算部1003より受け取ったスカラー倍点をもとにして復号化処理を行なう（ステップ2006）。その結果を復号化されたメッセージ1006として出力する（ステップ2007）。

## 【0117】

上記処理手順を図21のシーケンス図を用いて説明する。まず、復号部2101(図10の1002)の実行する処理について説明する。復号部2101は、入力メッセージを受け取る。復号部2101は、入力メッセージをもとに橜円曲線上の点を選び、スカラー倍計算部2102に橜円曲線上の点を与え、そしてスカラー倍計算部2102からスカラー倍点を受け取る。復号部2101は、受け取ったスカラー倍点を用いて復号化処理を行ない、その結果を出力メッセージとして出力する。

## 【0118】

次にスカラー倍計算部2102(図10の1003)の実行する処理について説明する。スカラー倍計算部2102は、復号部2101より橜円曲線上の点を受け取る。スカラー倍計算部2102は、秘密情報格納部2103よりスカラー値を受け取る。スカラー倍計算部2103は、受け取った橜円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、復号部2101にスカラー倍点を送る。

## 【0119】

最後に秘密情報格納部2103(図10の1004)の実行する処理について説明する。秘密情報格納部2103は、スカラー倍計算部2102がスカラー倍を計算できるように、スカラー値をスカラー倍計算部2102に送る。

## 【0120】

スカラー倍計算部1003が実行するスカラー倍計算は、上述した第1～第7実施例で説明したものがそのまま適用される。したがって、このスカラー倍計算は、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため復号部1002において、復号化処理を行なう際に復号化処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部1003のみであり、秘密情報に関する情報は漏洩しない。

## 【0121】

【発明の効果】

以上述べたように、本発明によれば、暗号処理システムにおける秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても、暗号処理経過と秘密情報との依存関係が完全に断ち切られているので、秘密情報は漏洩しない。また、使用する楕円曲線をモンゴメリ型楕円曲線とすることで暗号処理の高速化を図ることができる。同様に、楕円曲線として標数2の有限体上で定義された楕円曲線を用いることで暗号処理の高速化を図ることができる。

【図面の簡単な説明】

【図1】

本発明の第1実施例のスカラー倍計算方法を示すフローチャート図である。

【図2】

第1実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図3】

本発明の実施の形態に係る署名作成装置の構成図である。

【図4】

本発明の第2実施例のスカラー倍計算方法を示すフローチャート図である。

【図5】

第2実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図6】

本発明の第3実施例のスカラー倍計算方法を示すフローチャート図である。

【図7】

第3実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図8】

本発明の第4実施例のスカラー倍計算方法を示すフローチャート図である。

【図9】

第4実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図10】

本発明の実施の形態に係る復号化装置の構成図である。

【図11】

本発明の実施の形態に係る暗号処理システムの構成図である。

【図12】

本発明の第5実施例のスカラー倍計算方法を示すフローチャート図である。

【図13】

本発明の第5実施例のスカラー倍計算方法を示すフローチャート図である。

【図14】

本発明の第5実施例のスカラー倍計算方法を示すフローチャート図である。

【図15】

第5実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図16】

図11の暗号処理システムにおける暗号処理方法を示すフローチャート図である。

【図17】

図11の暗号処理システムにおける処理の流れを示すシーケンス図である。

【図18】

図3の署名作成装置における署名作成方法を示すフローチャート図である。

【図19】

図3の署名作成装置における処理の流れを示すシーケンス図である。

【図20】

図10の復号化装置における復号化方法を示すフローチャート図である。

【図21】

図10の復号化装置での処理の流れを示すシーケンス図である。

【図22】

本発明の第6実施例のスカラー倍計算方法を示すフローチャート図である。

【図23】

本発明の第6実施例のスカラー倍計算方法を示すフローチャート図である。

【図24】

本発明の第6実施例のスカラー倍計算方法を示すフローチャート図である。

【図25】

第6実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図26】

本発明の第7実施例のスカラー倍計算方法を示すフローチャート図である。

【図27】

第7実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

【図28】

図27のランダム化射影座標変換装置を示す図である。

【図29】

ランダム化射影座標変換装置におけるランダム化射影座標変換方法を示すフローチャート図である。

【符号の説明】

201 スカラー倍計算装置

202 点格納部

203 加算演算部

204 2倍算演算部

205 ピット値判定部

206 繰り返し判定部

207 点及びスカラー値

208 スカラー倍

301 署名作成装置

302 署名部

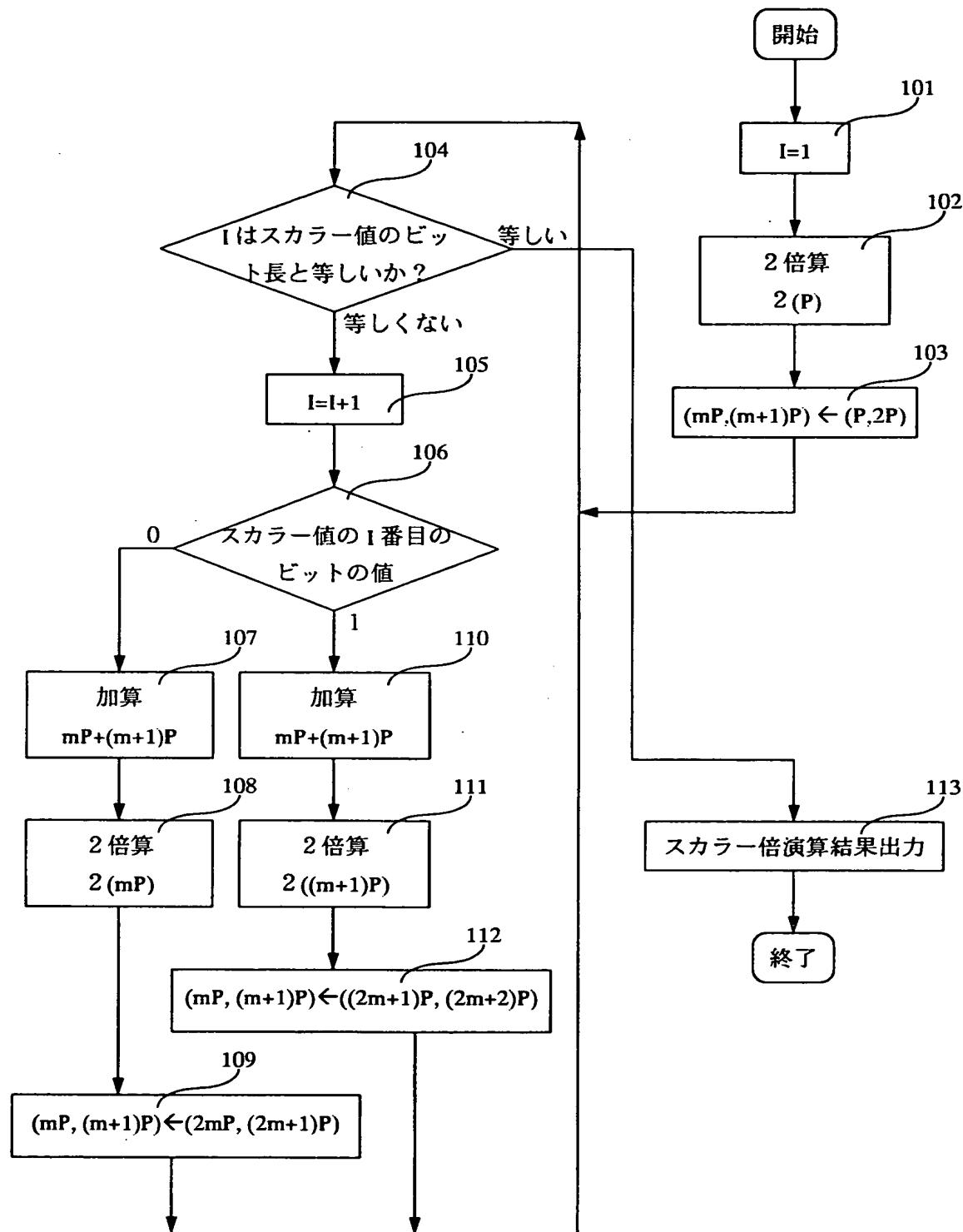
303 スカラー倍計算部

304 秘密情報格納部  
305 入力メッセージ  
306 出力メッセージ  
701 スカラー倍計算装置  
702 点格納部  
703 加算及び2倍算演算部  
704 2倍算演算部  
705 ビット値判定部  
706 繰り返し判定部  
707 点及びスカラー値  
708 スカラー倍  
1001 復号化装置  
1002 復号化部  
1003 スカラー倍計算部  
1004 秘密情報格納部  
1005 入力メッセージ  
1006 出力メッセージ  
1101 暗号処理システム  
1102 暗号処理部  
1103 スカラー倍計算部  
1104 秘密情報格納部  
1105 入力メッセージ  
1106 出力メッセージ  
1501 スカラー倍計算装置  
1502 点格納部  
1503 加算演算部  
1504 2倍算演算部  
1505 ビット値判定部  
1506 繰り返し判定部

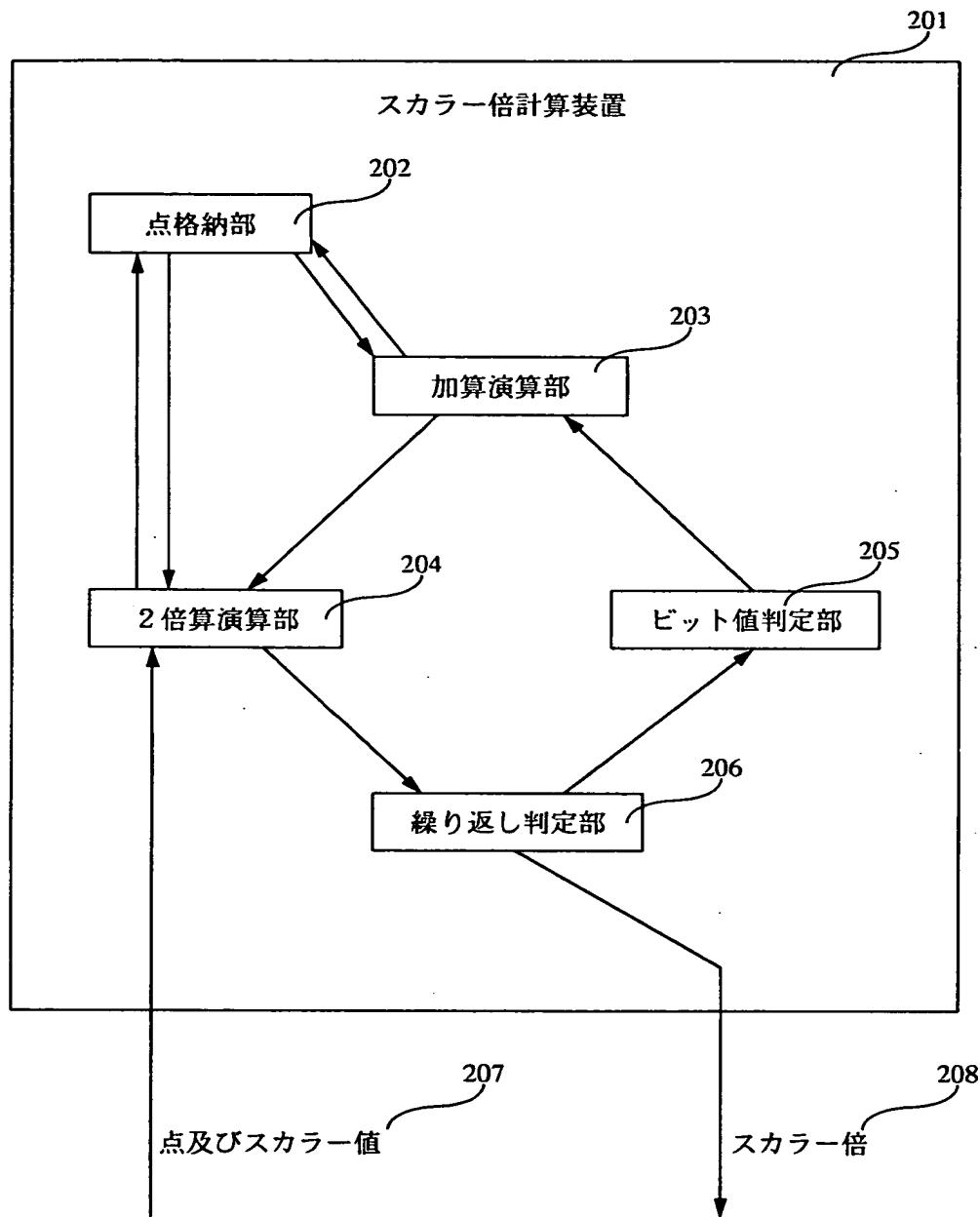
- 1507 点及びスカラー値
- 1508 スカラー倍
- 1509 演算ランダム化部
- 2701 スカラー倍計算装置
- 2702 点格納部
- 2703 加算演算部
- 2704 2倍算演算部
- 2705 ビット値判定部
- 2706 繰り返し判定部
- 2707 点及びスカラー値
- 2708 スカラー倍
- 2709 ランダム化射影座標変換部
- 2801 ランダム化射影座標変換装置
- 2802 座標判定部
- 2803 亂数生成部
- 2804 射影座標変換部
- 2805 楕円曲線上の点
- 2806 ランダム化射影座標で表された点

【書類名】 図面

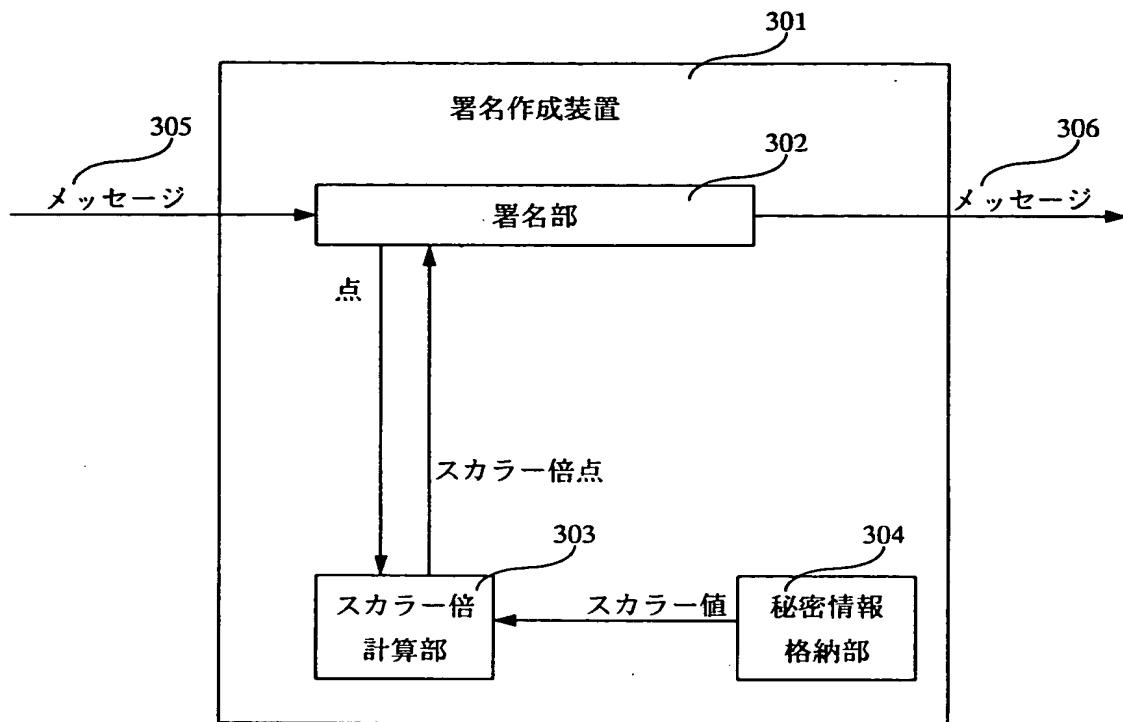
【図1】



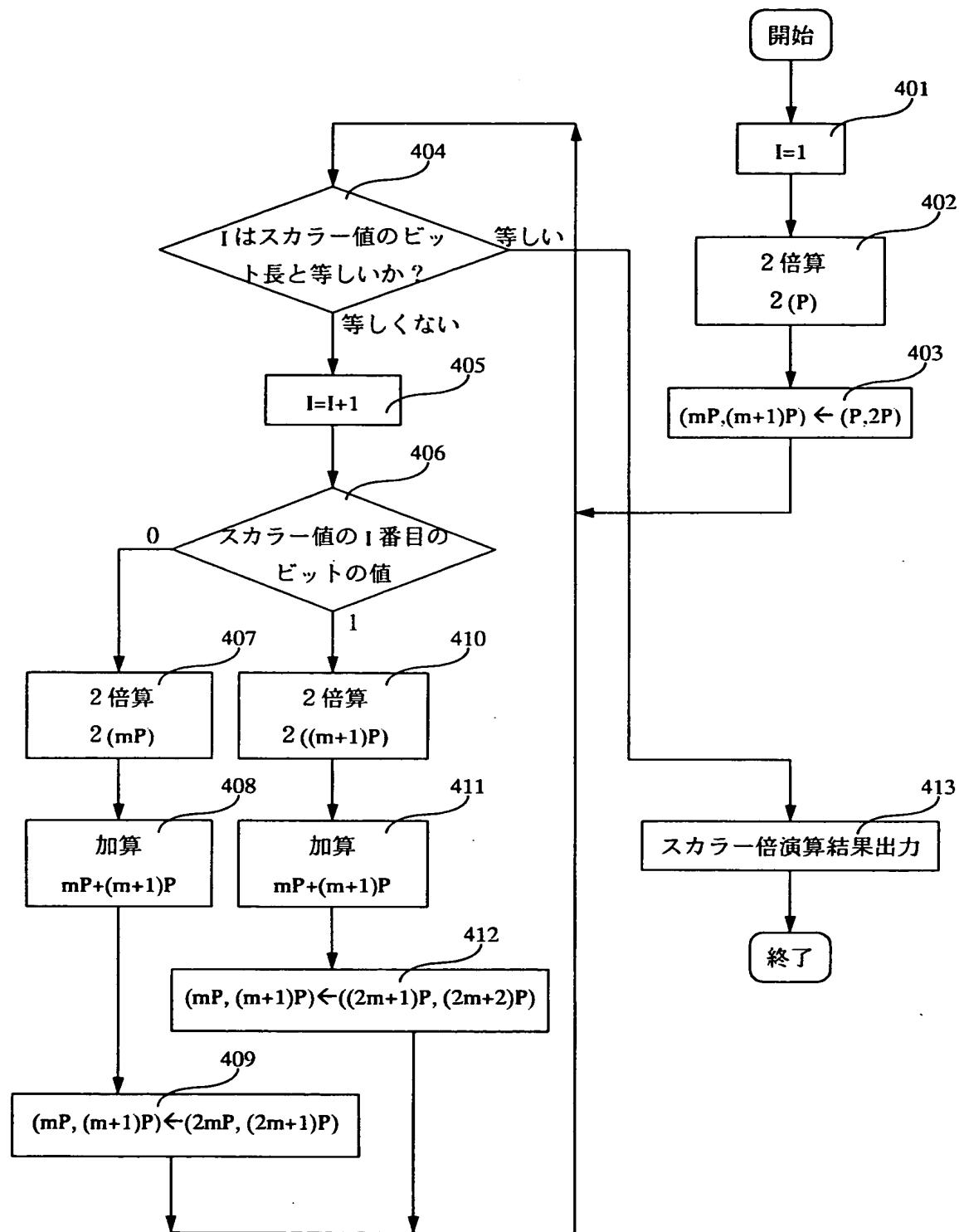
【図2】



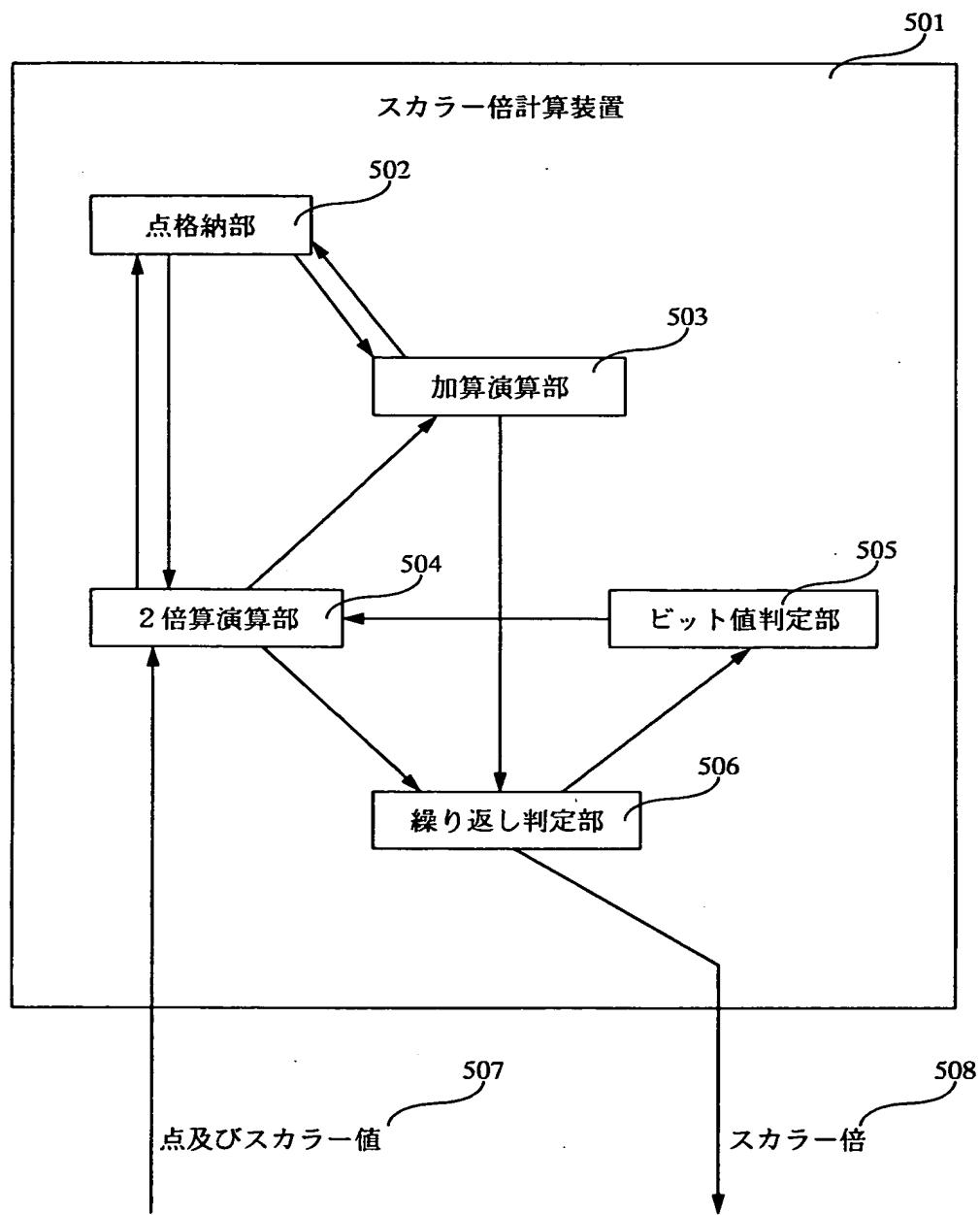
【図3】



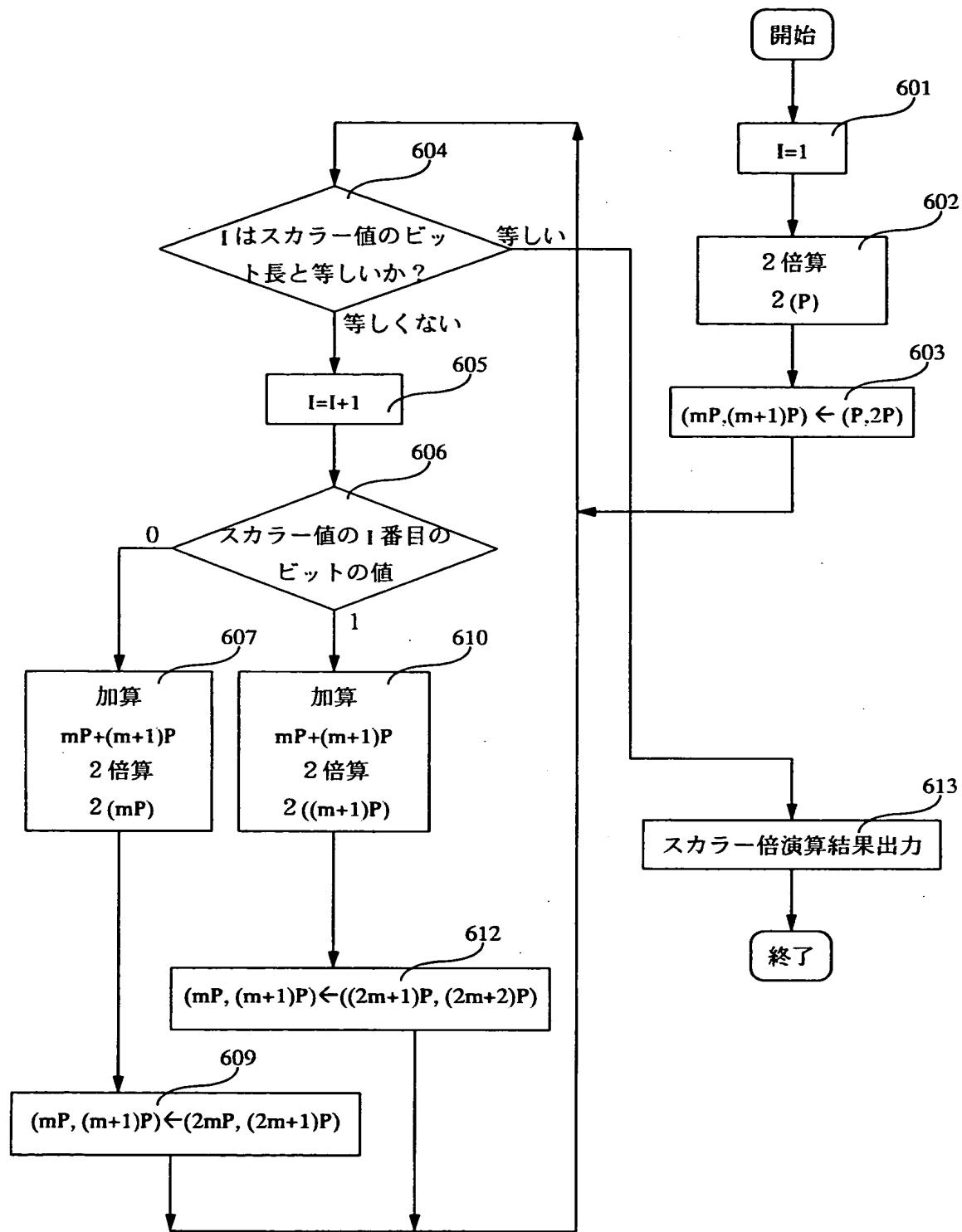
【図4】



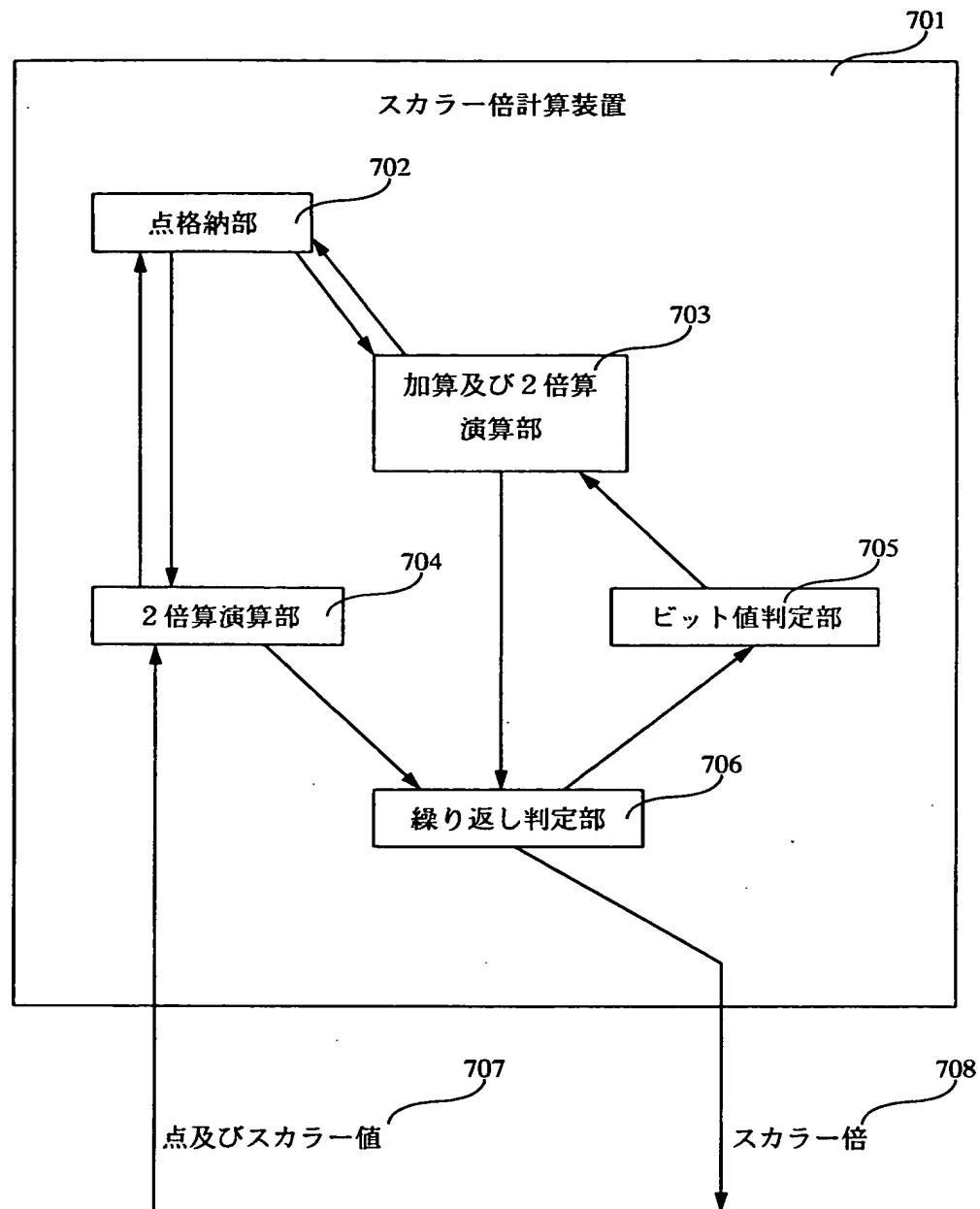
【図5】



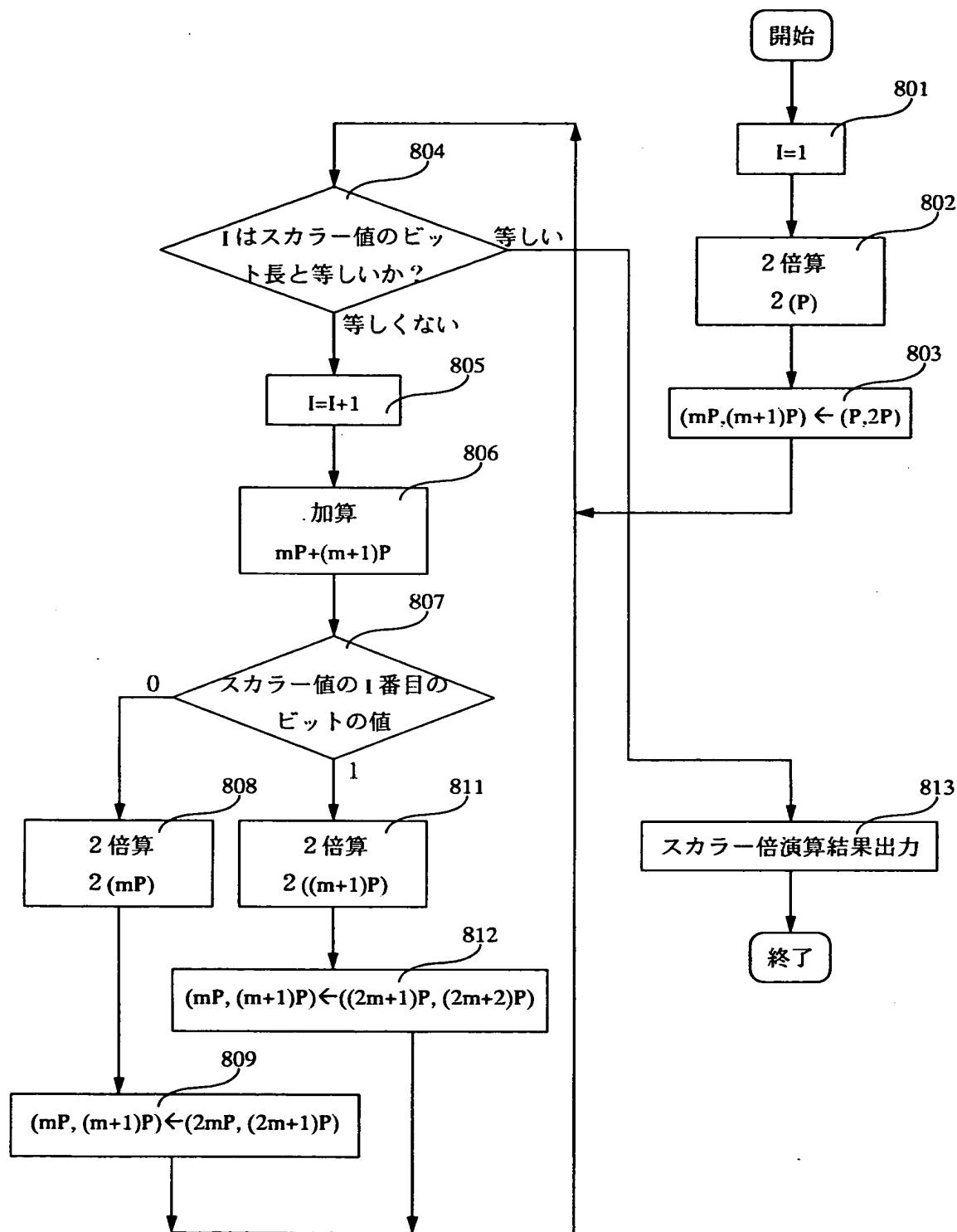
【図6】



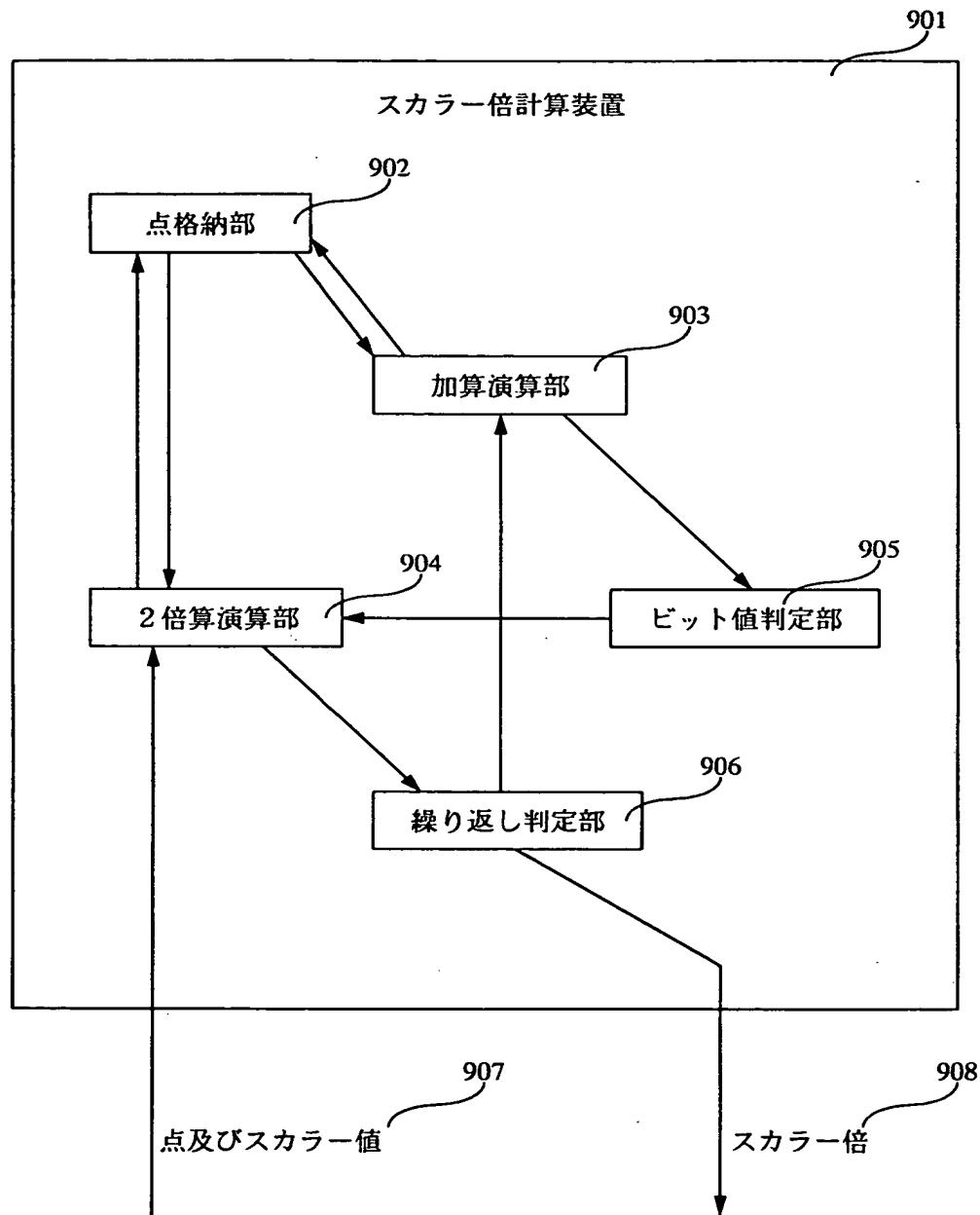
【図7】



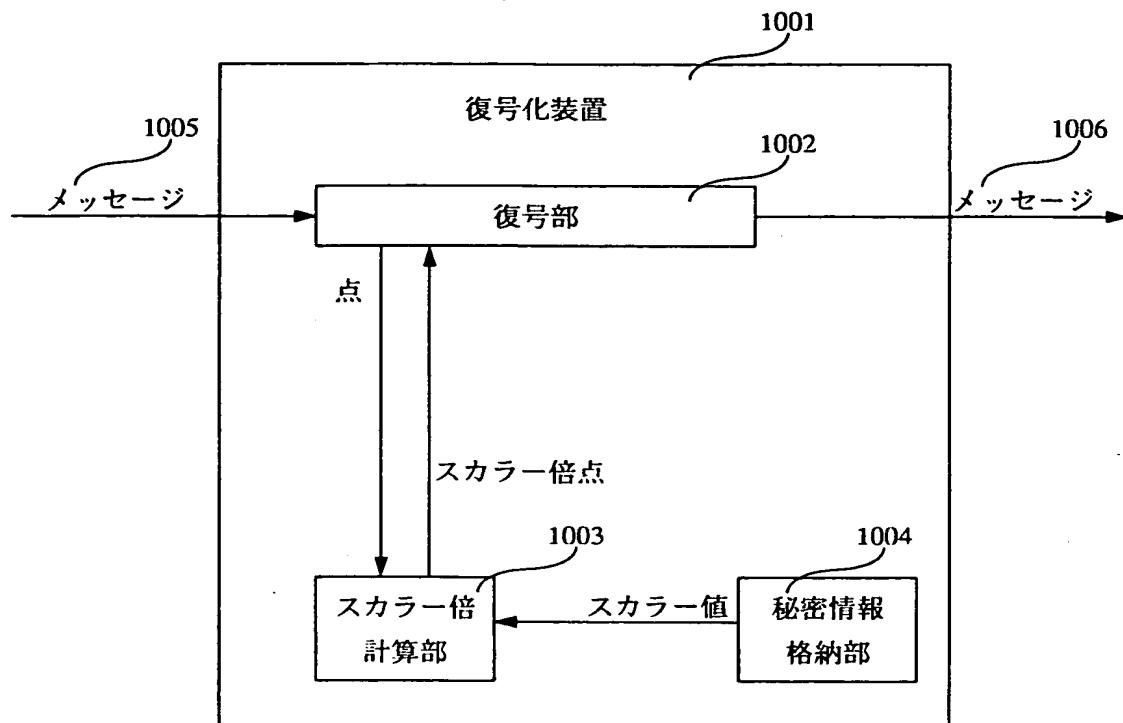
【図8】



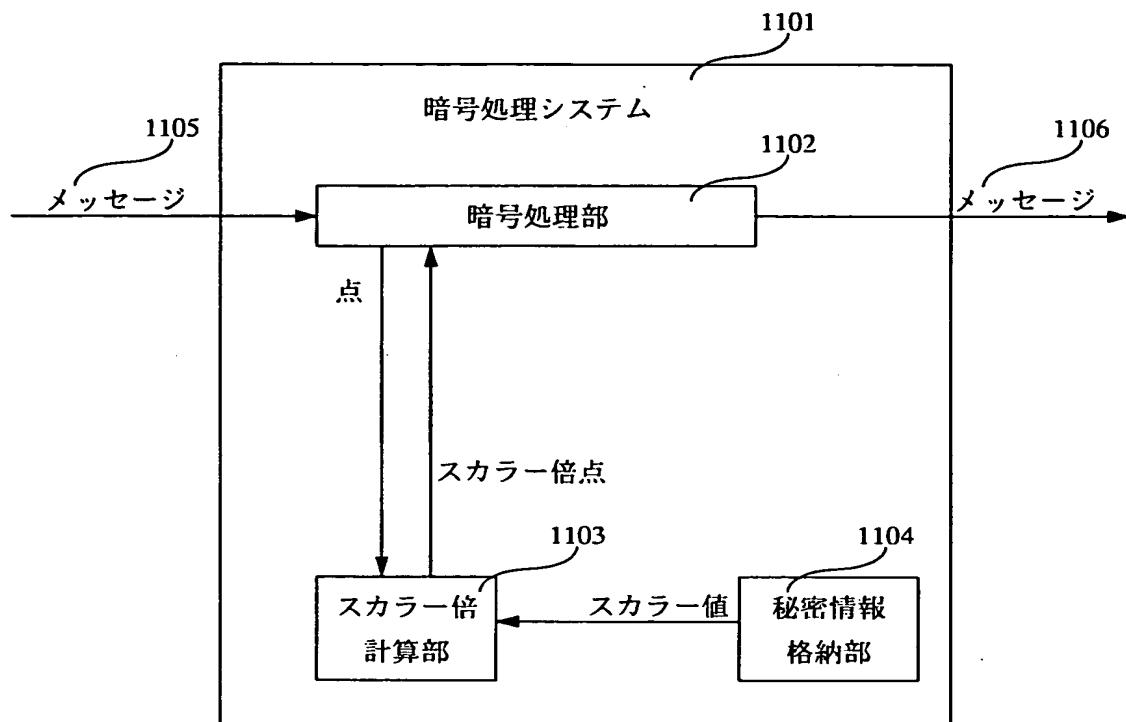
【図9】



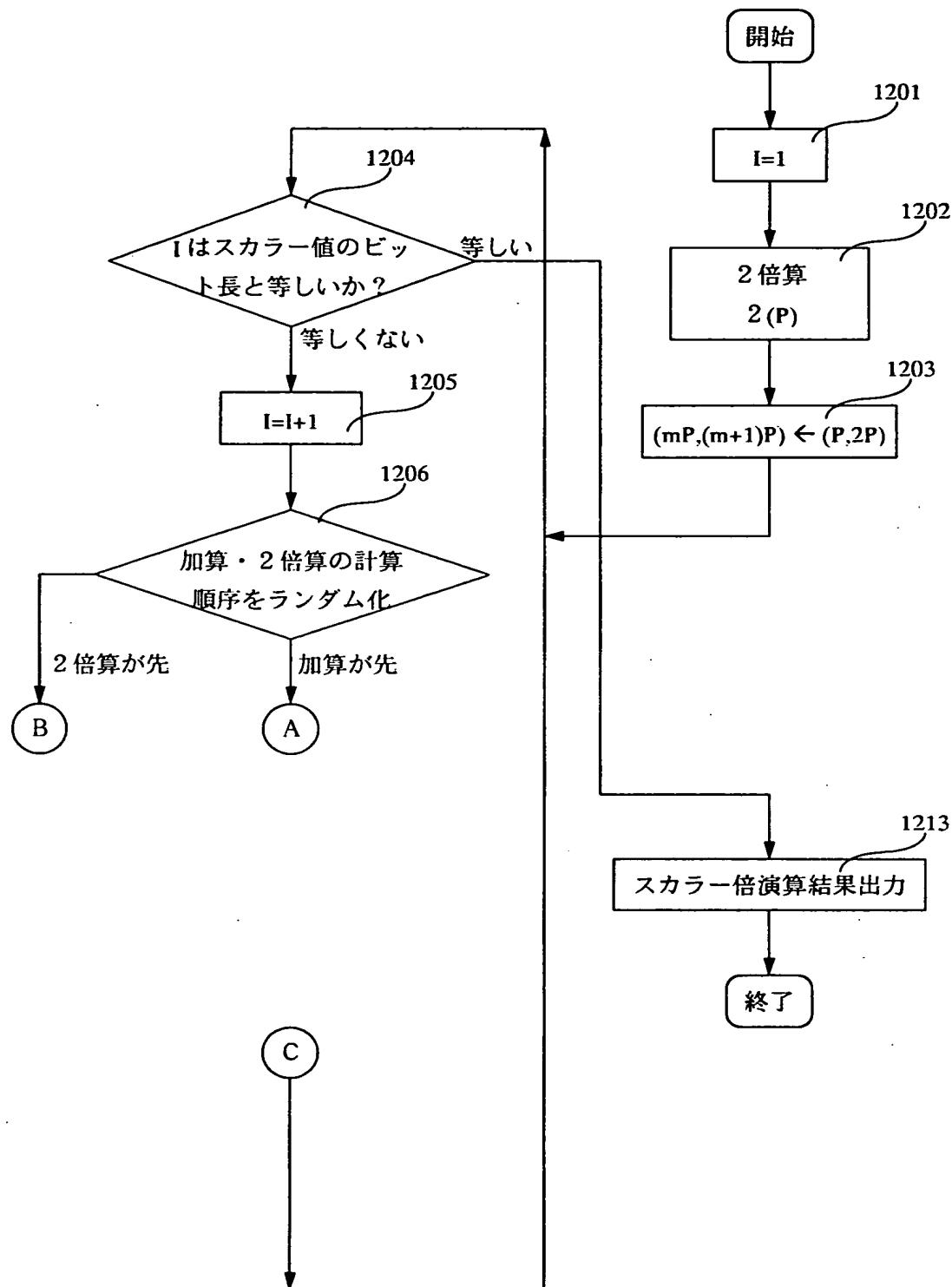
【図10】



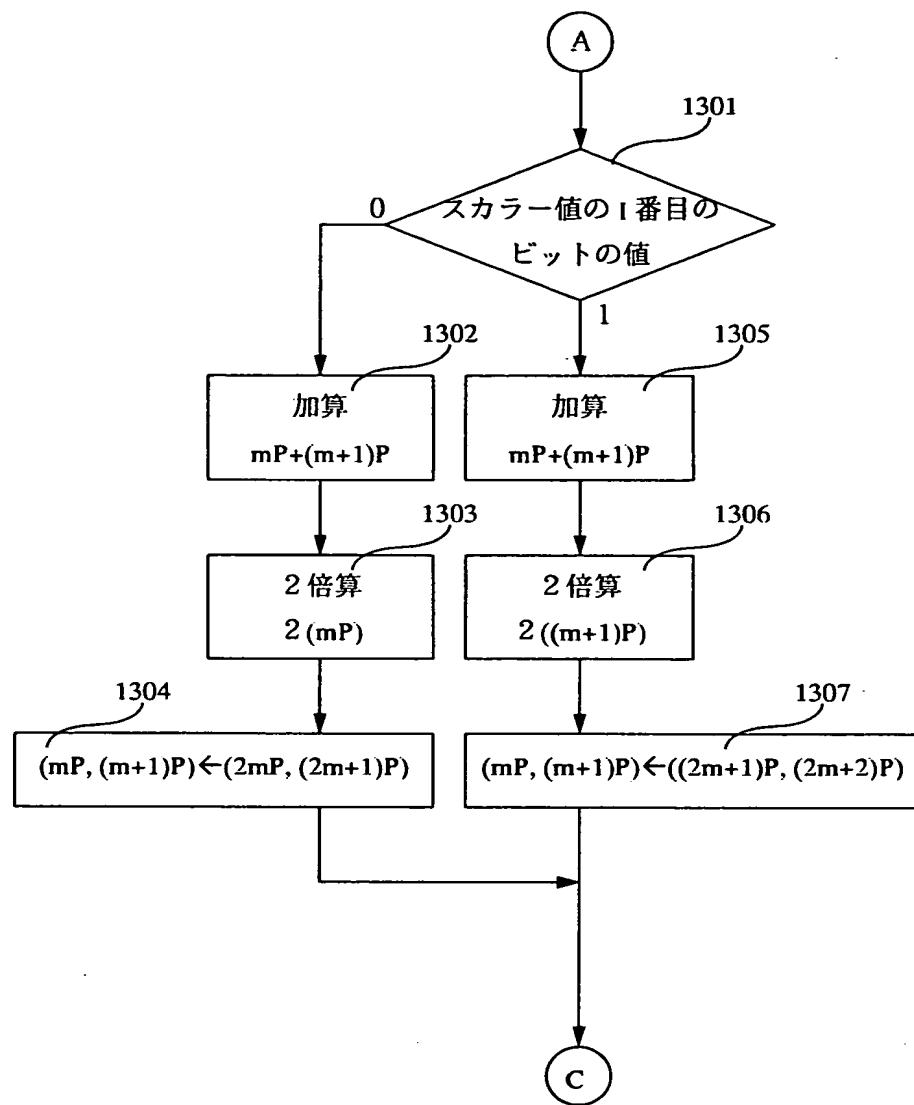
【図11】



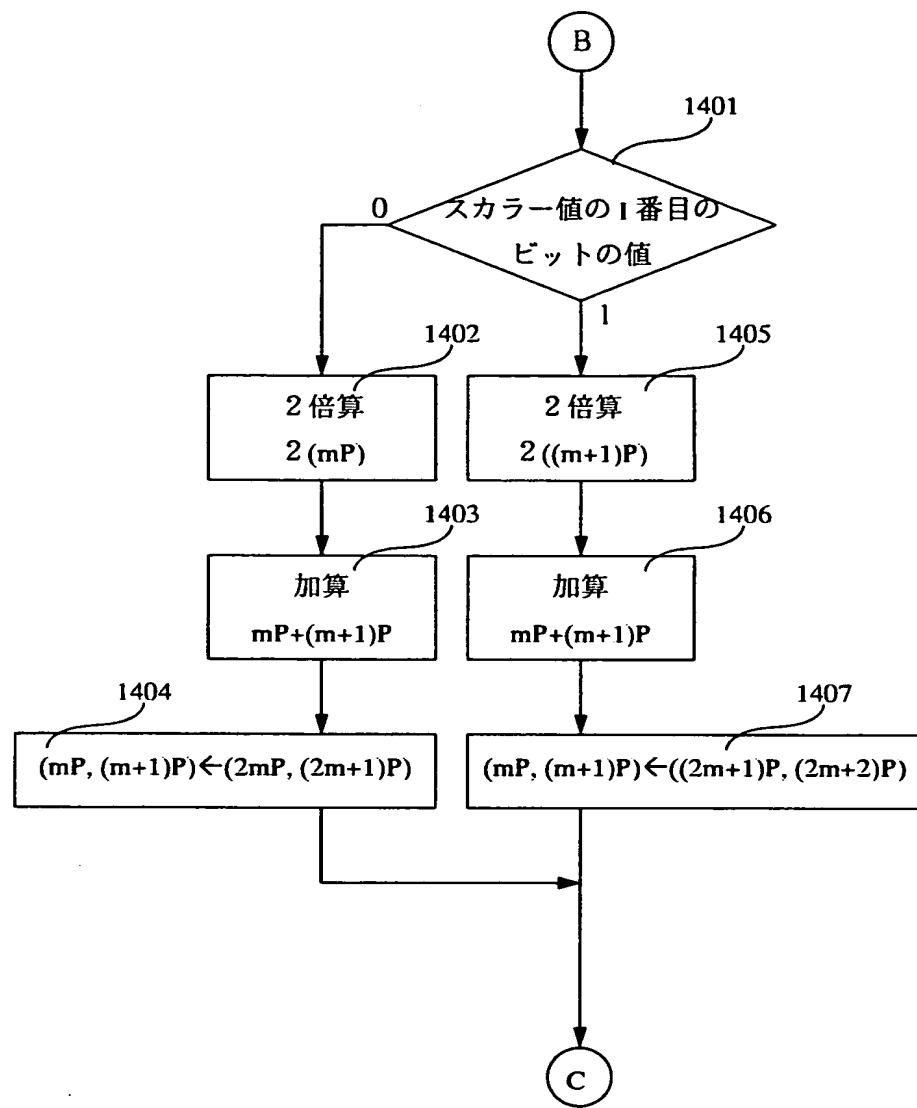
【図12】



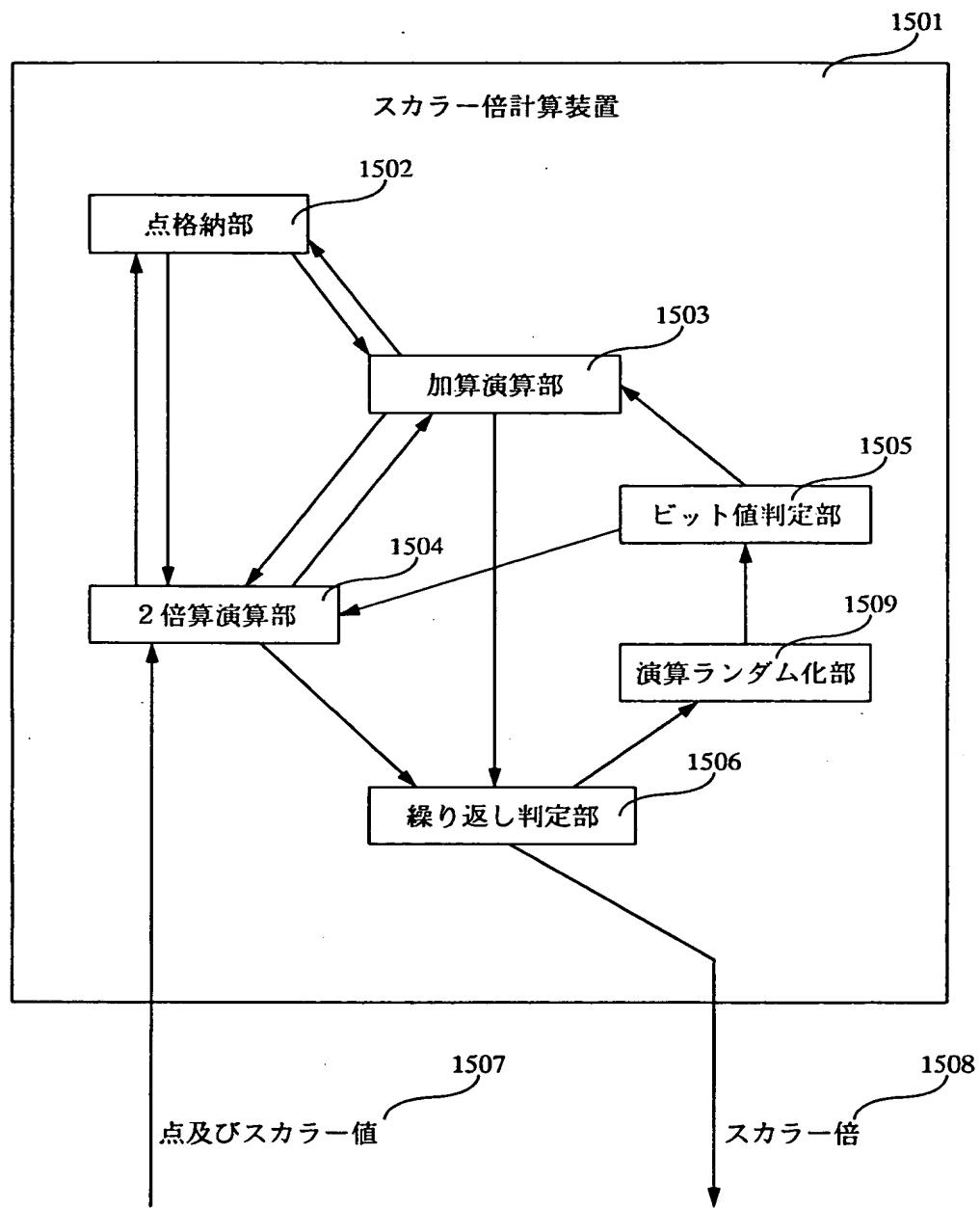
【図13】



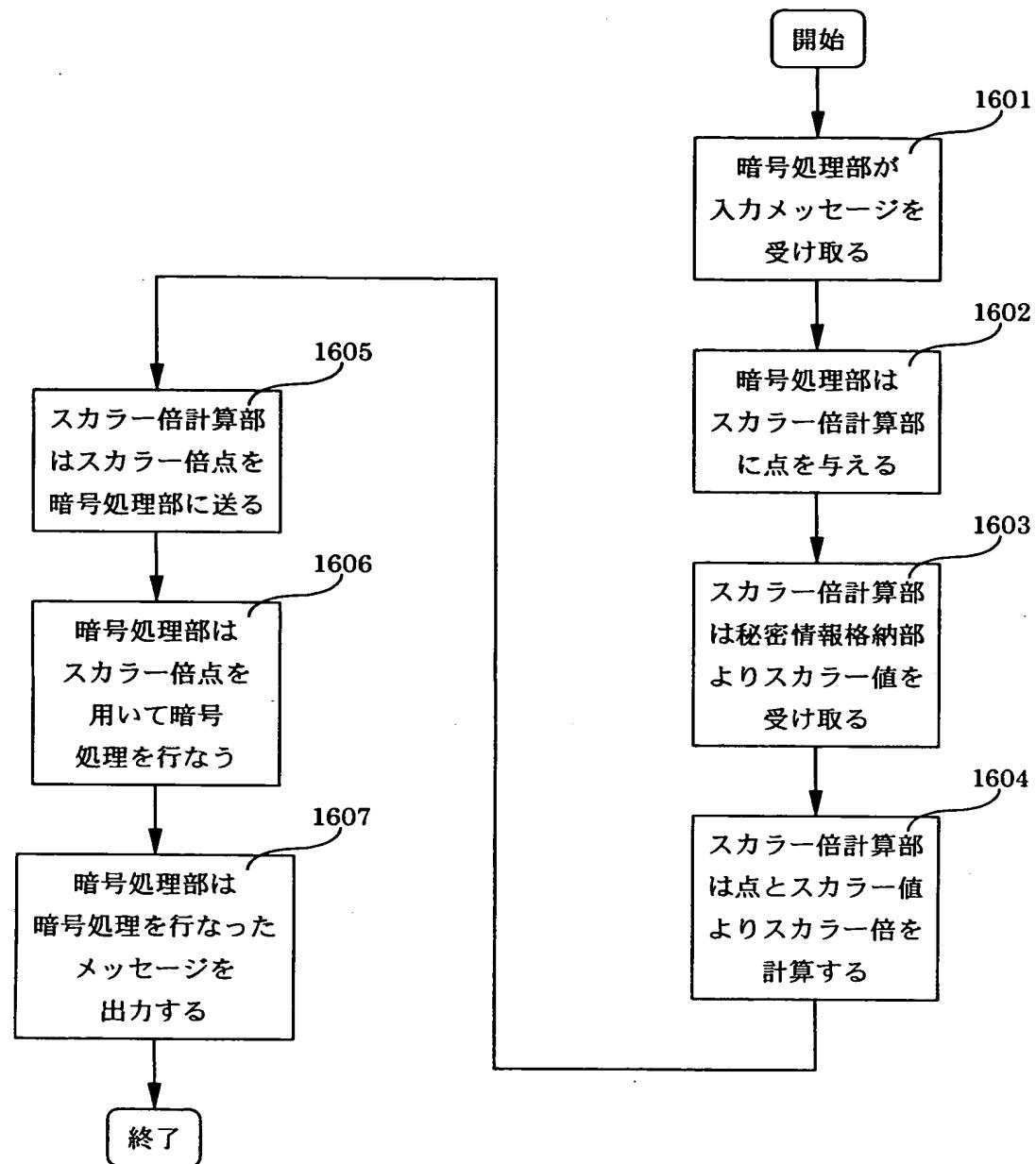
【図14】



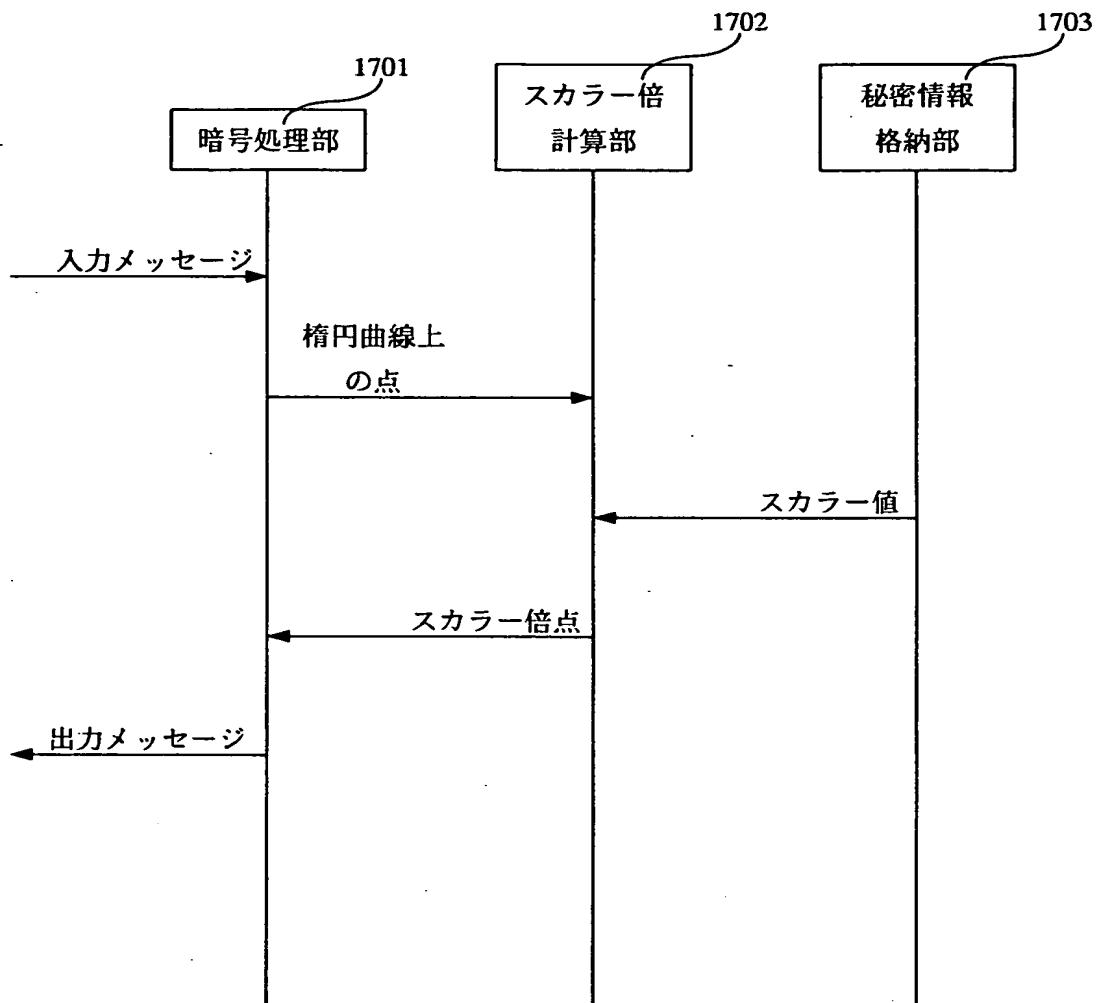
【図15】



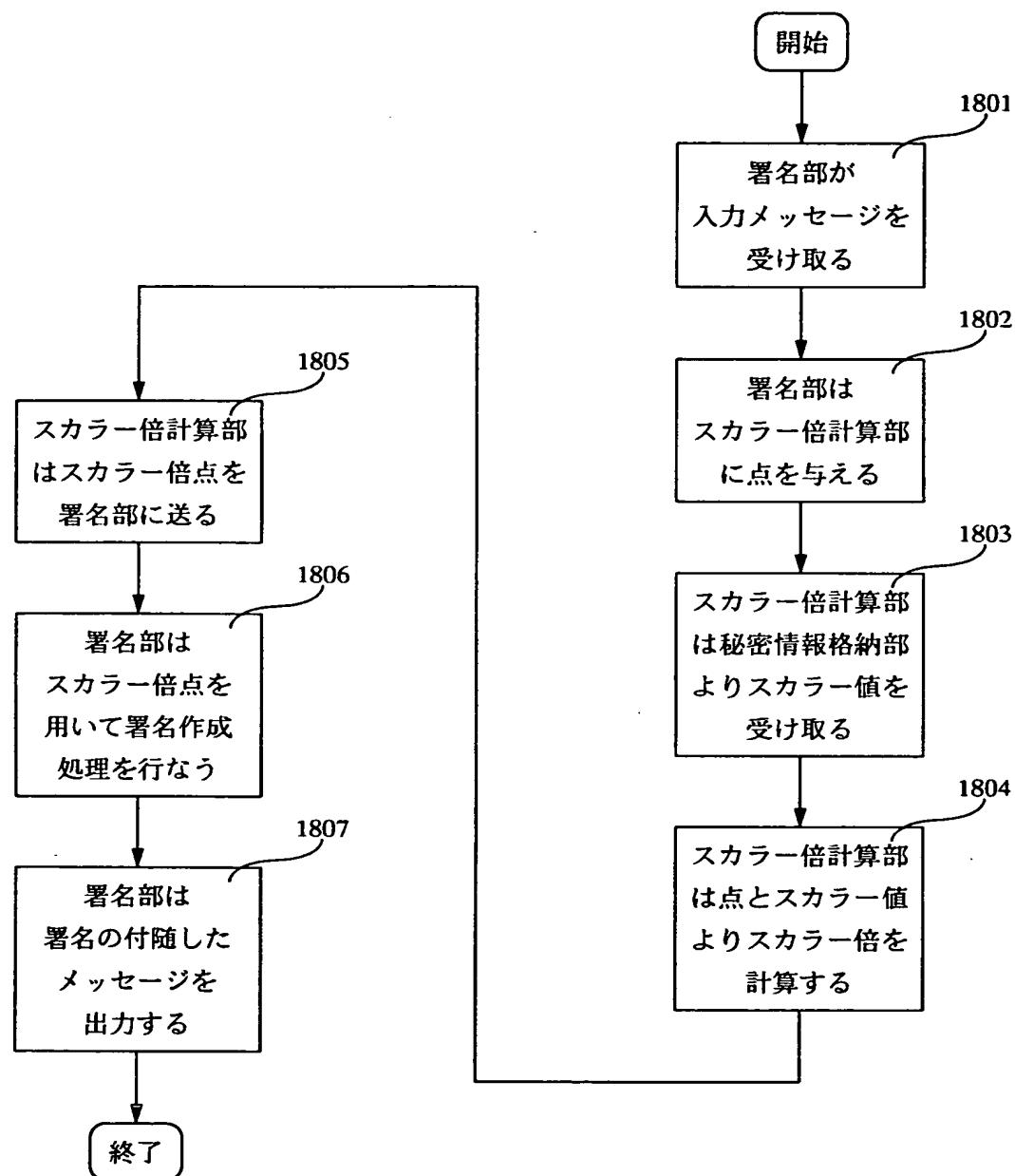
【図16】



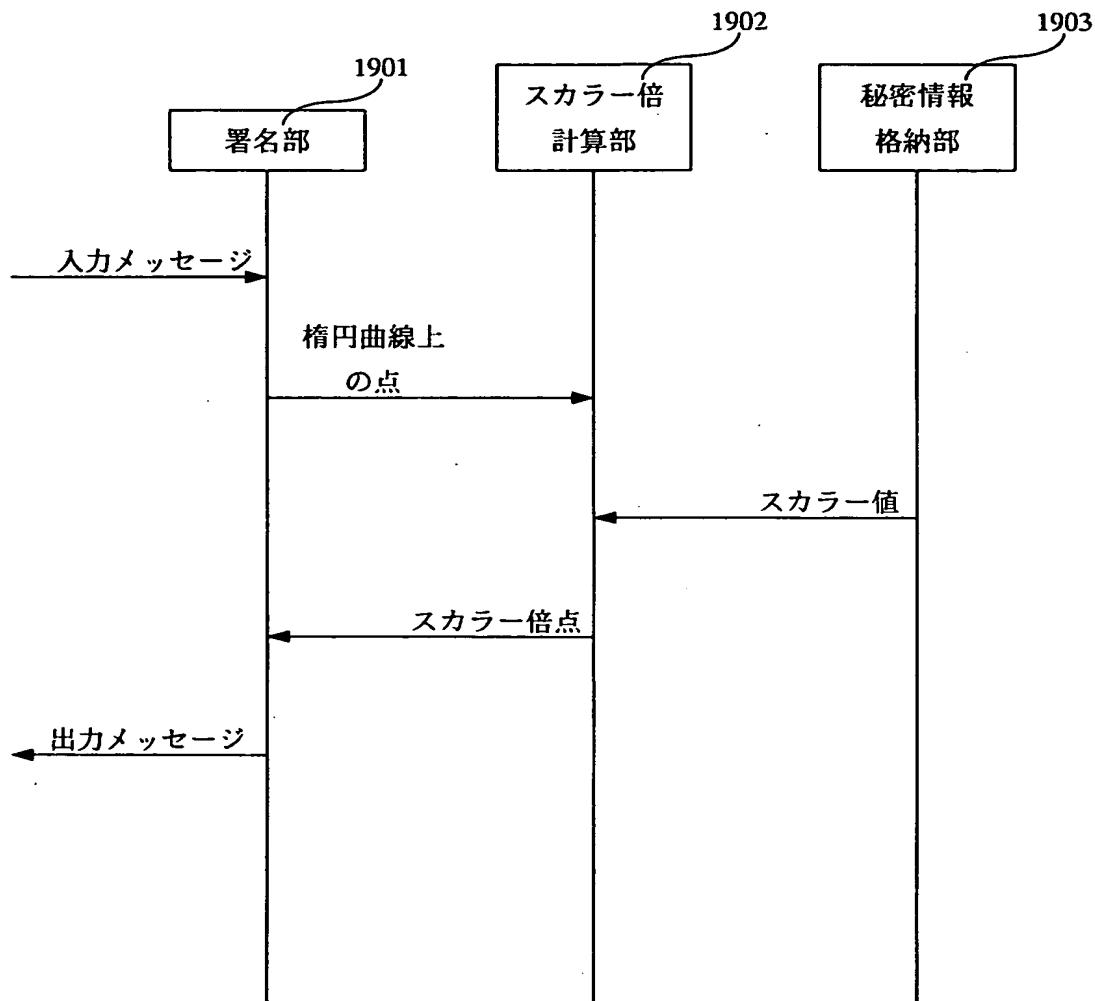
【図17】



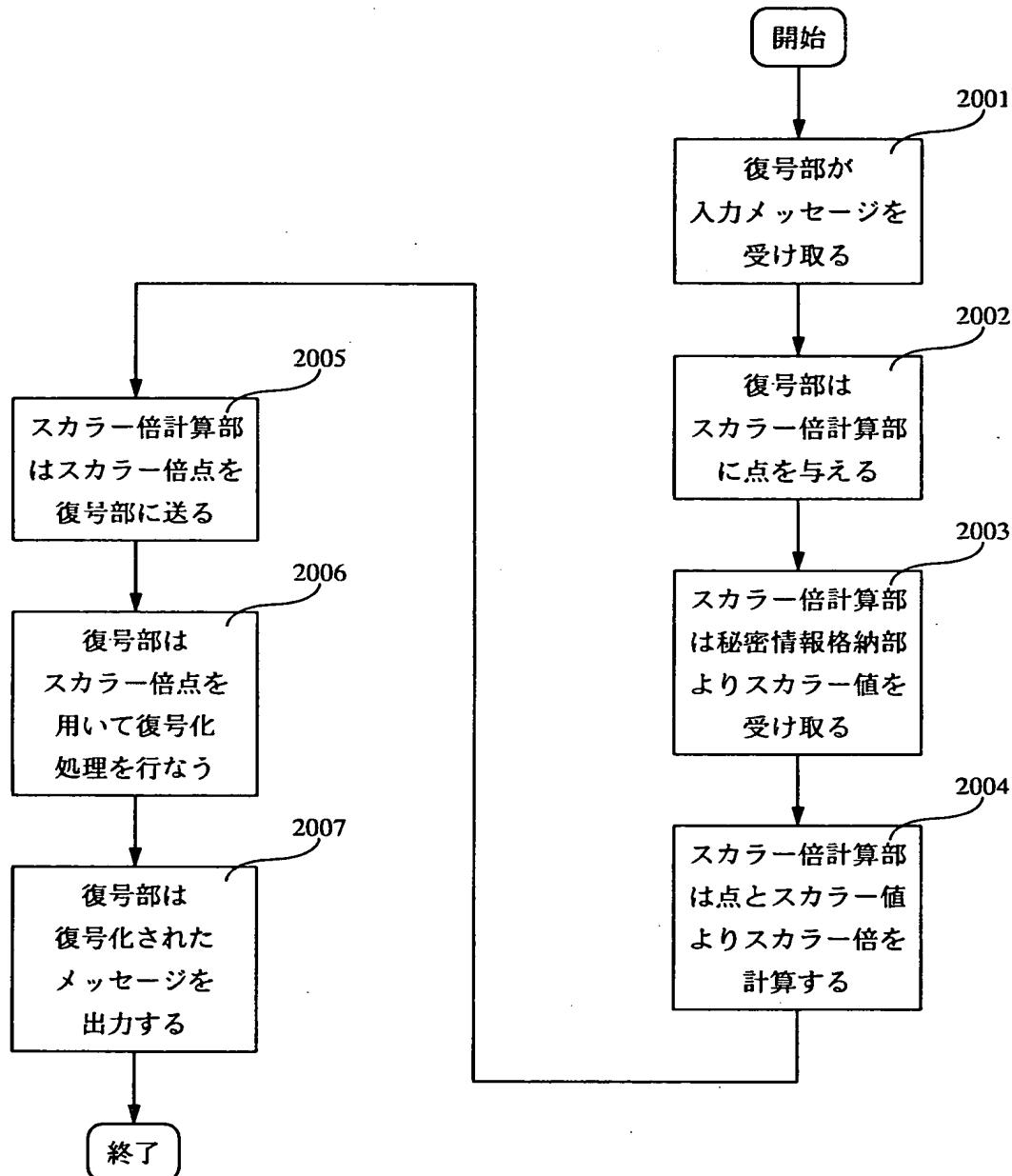
【図18】



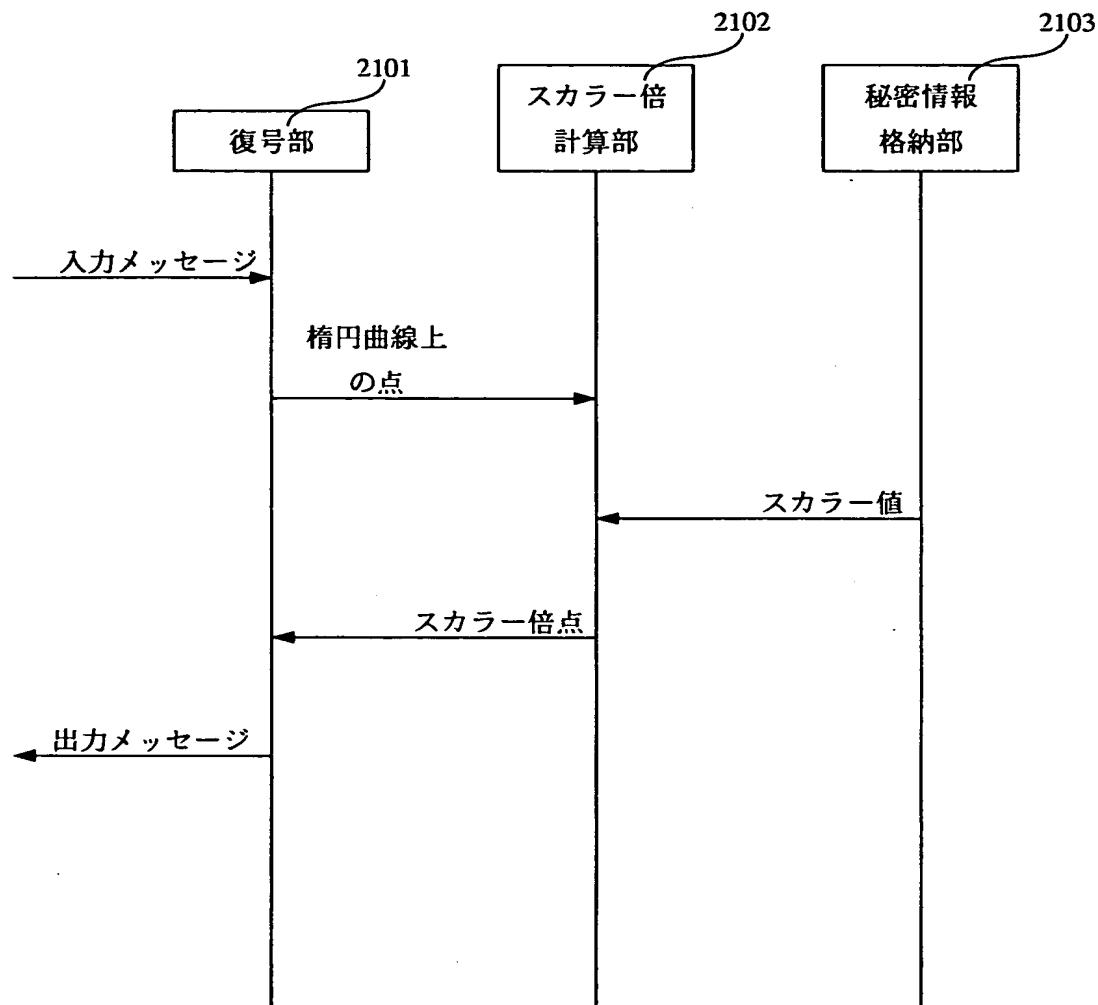
【図19】



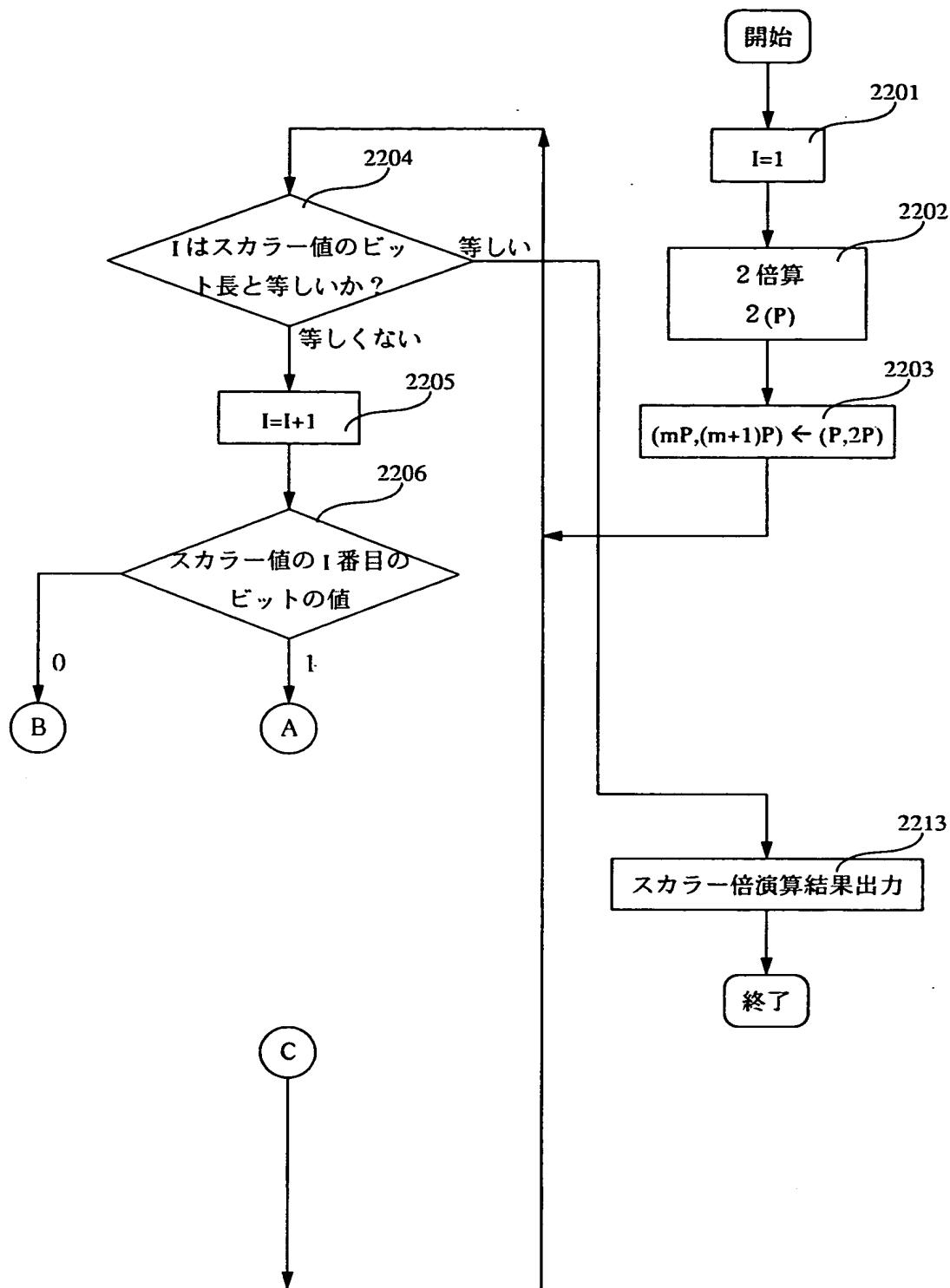
【図20】



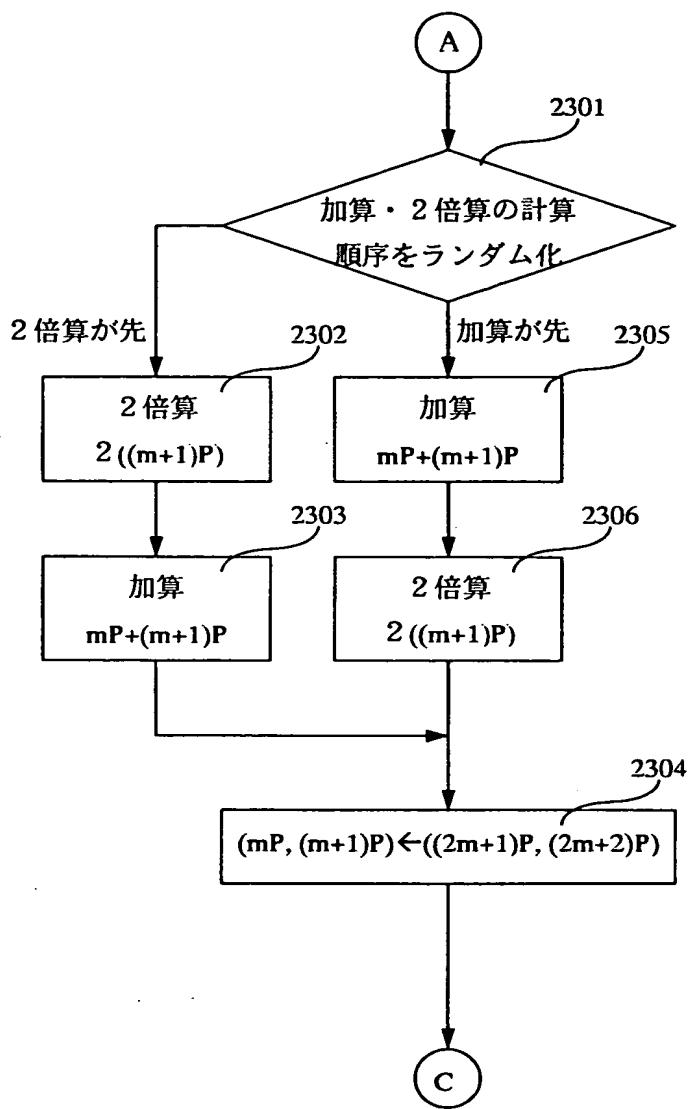
【図21】



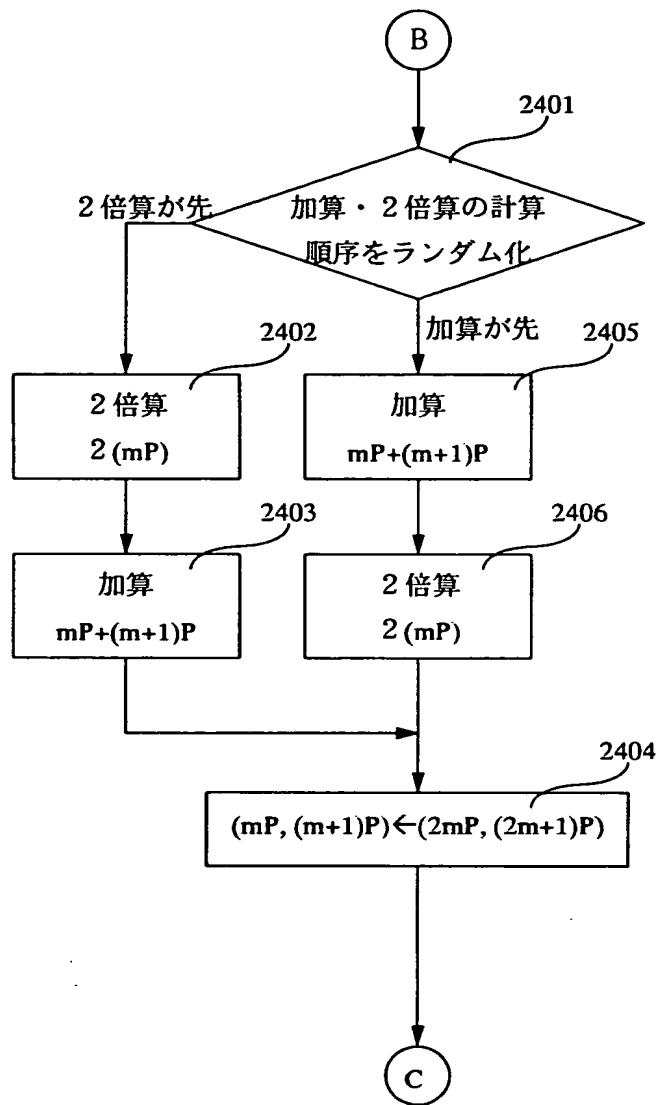
【図22】



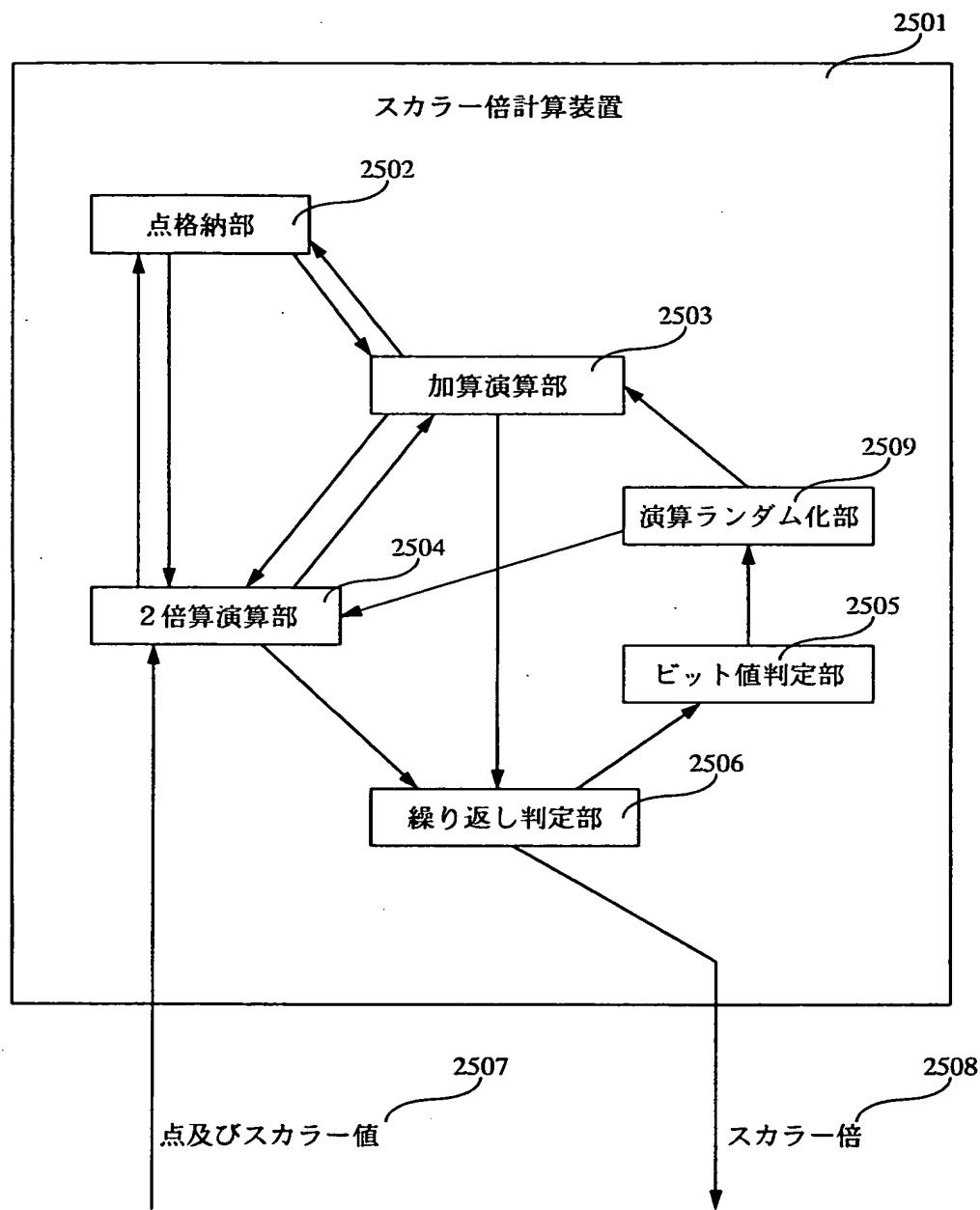
【図23】



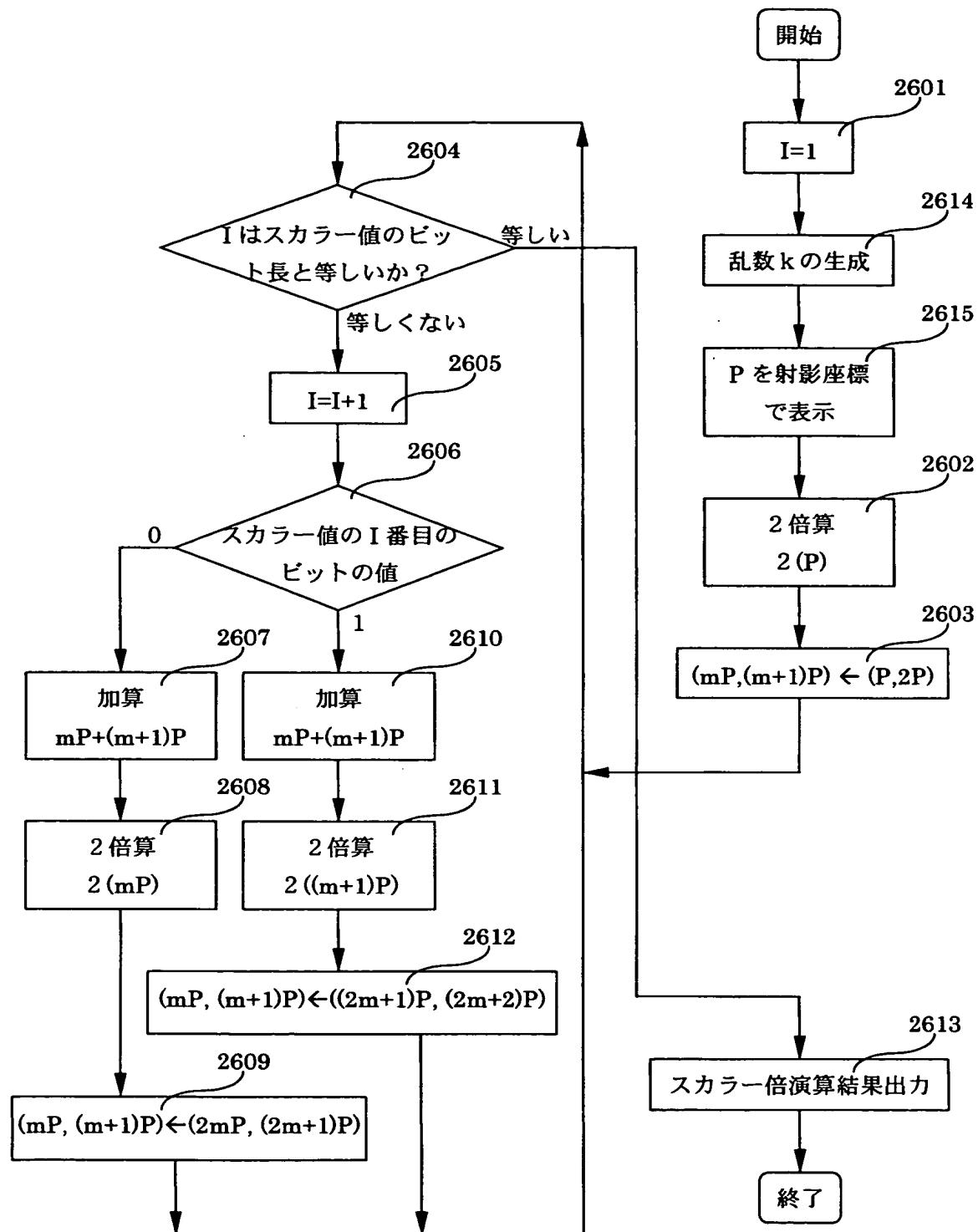
【図24】



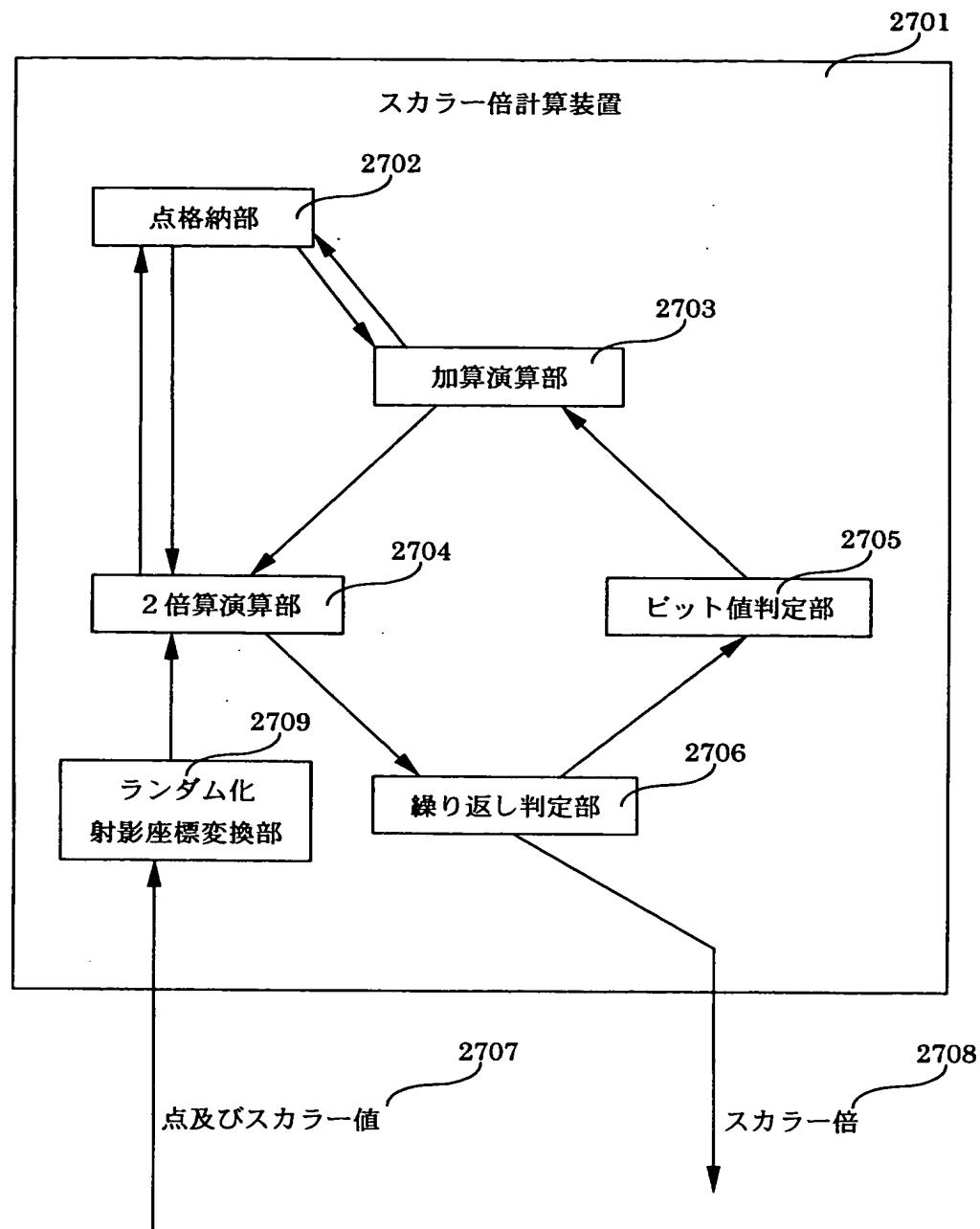
【図25】



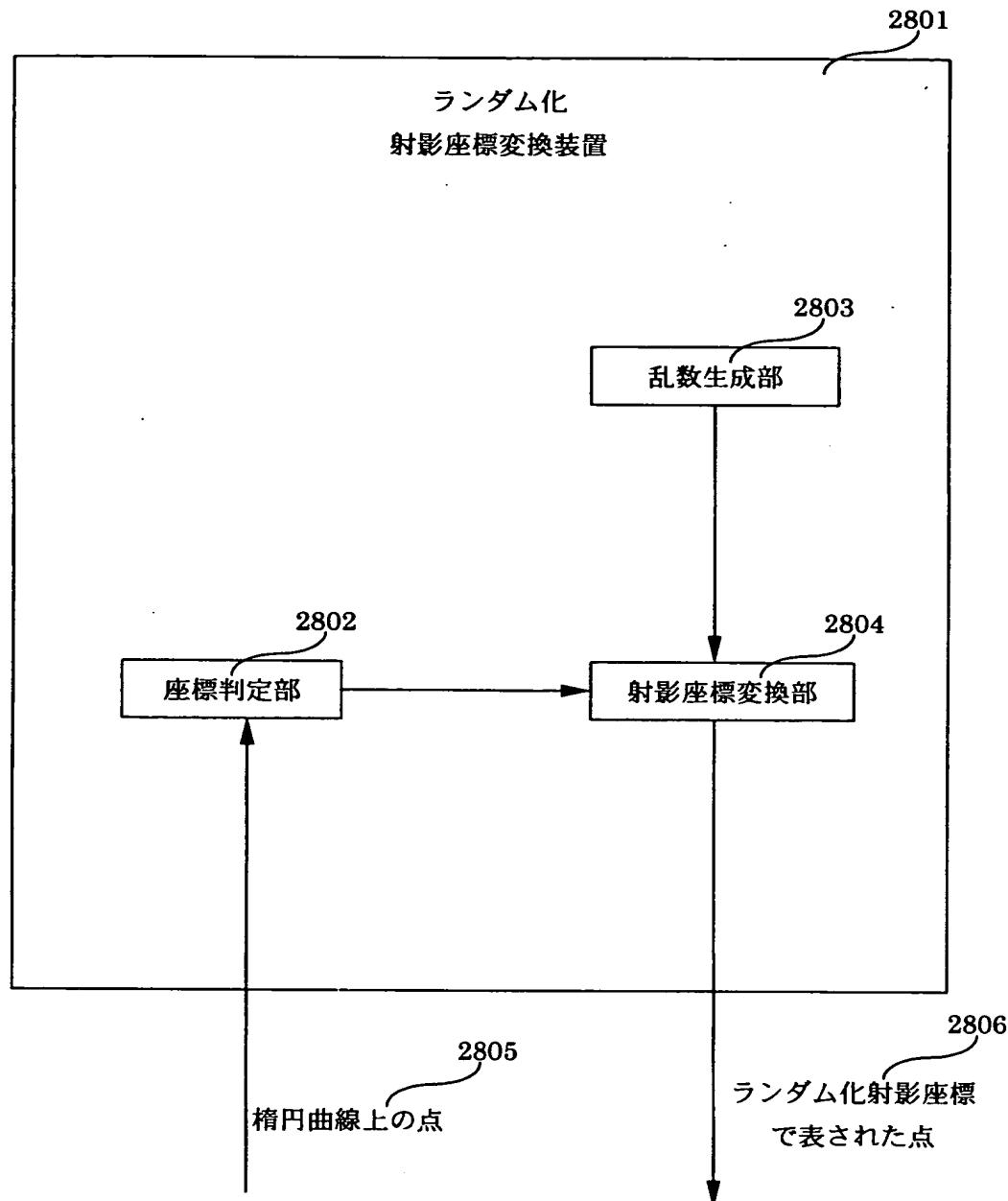
【図26】



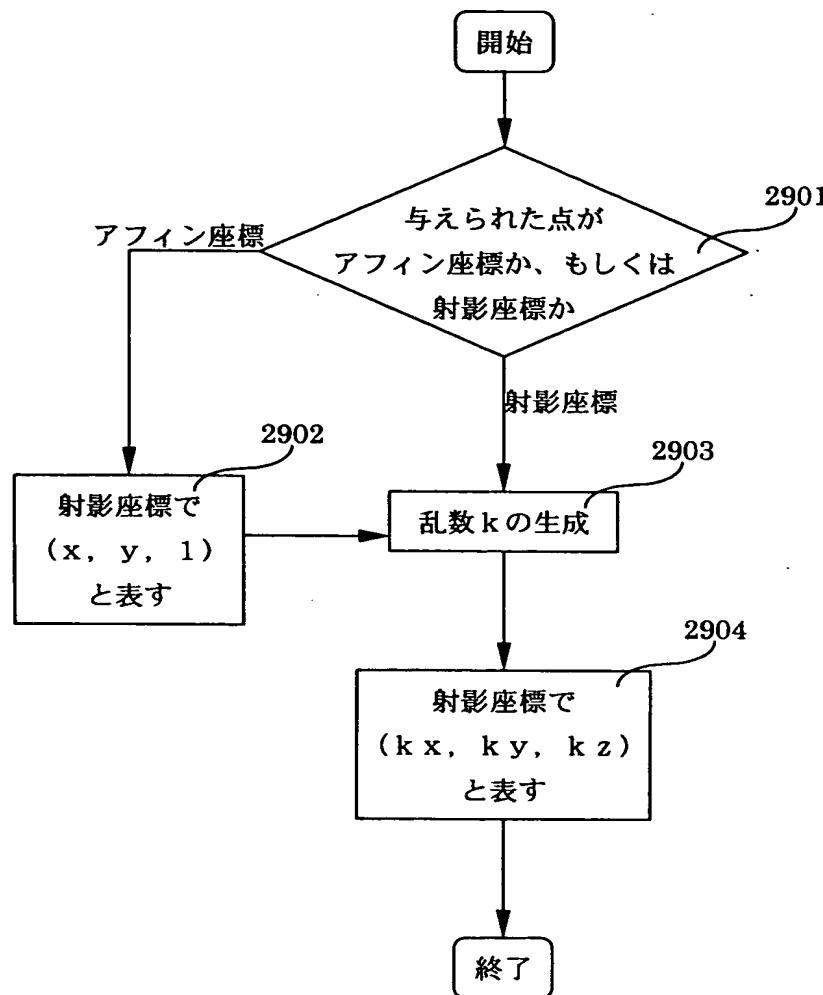
【図27】



【図28】



【図29】



【書類名】 要約書

【要約】

【課題】

楕円曲線暗号における秘密情報を用いた暗号処理において、DPA等のパワーハナリシスという攻撃法により、暗号処理経過から秘密情報が復元される可能性があった。本発明の目的は、パワーハナリシスにより暗号処理経過が漏洩しても、秘密情報自体は漏洩せず、しかも高速に暗号処理を実行できる暗号処理方法を提供することにある。

【解決手段】

暗号処理経過と秘密情報との依存関係を断ち切った暗号処理方法を与える。特に、秘密情報であるスカラー値に対して、スカラー倍計算経過がそれらの値に依存しないスカラー倍計算方法を与える。すなわち、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算する際、スカラー値のビットの値を判定し、その判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行する。

【選択図】 図2

認定・付加情報

特許出願の番号	特願2000-160001
受付番号	50000667141
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 5月31日

<認定情報・付加情報>

【提出日】 平成12年 5月30日

次頁無

出願人履歴情報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所

く。

### 【0070】

ステップ1302として、加算演算部1503により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1303へ行く。ステップ1303として、2倍算演算部1504により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ1304へ行く。ステップ1304として、ステップ1303で求めた点 $2mP$ とステップ1302で求めた点 $(2m+1)P$ を点格納部1502に点の組( $2mP, (2m+1)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ1204へ戻る。

### 【0071】

ステップ1305として、加算演算部1503により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1306へ行く。ステップ1306として、2倍算演算部1504により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ1307へ行く。ステップ1307として、ステップ1305で求めた点 $(2m+1)P$ とステップ1306で求めた点 $(2m+2)P$ を点格納部1502に点の組( $(2m+1)P, (2m+2)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ1204へ戻る。

### 【0072】

ステップ1401として、ビット値判定部1505により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ1402へ行く。そのビットの値が1であればステップ1405へ行く。

### 【0073】

ステップ1402として、2倍算演算部1504により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ の2倍算2( $mP$ )を行ない、点 $2mP$ を計算する。その後ステップ1403へ行く。ステップ1403として、加算演算部1503により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1404へ行く。ステップ1404として、ステップ1402で求めた点 $2mP$ とステップ1403で求めた点 $(2m+1)P$ を点格納部1502に点の組( $2mP, (2m+1)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ1204へ戻る。

#### 【0074】

ステップ1405として、2倍算演算部1504により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $(m+1)P$ の2倍算2( $(m+1)P$ )を行ない、点 $(2m+2)P$ を計算する。その後ステップ1406へ行く。ステップ1406として、加算演算部1503により、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1407へ行く。ステップ1407として、ステップ1406で求めた点 $(2m+1)P$ とステップ1405で求めた点 $(2m+2)P$ を点格納部1502に点の組( $(2m+1)P, (2m+2)P$ )として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ1204へ戻る。

#### 【0075】

ステップ1213として、点格納部1502に格納されている点の組( $mP, (m+1)P$ )から、点 $mP$ をスカラー倍1508として出力し、終了する。

#### 【0076】

以上の手順により出力する値である点 $mP$ が点 $P$ のスカラー値 $d$ によるスカラ倍の点 $dP$ となることは、第1実施例の場合と同様に示すことができる。

#### 【0077】

また、橢円曲線としてモンゴメリ型橢円曲線を用いると、加算及び2倍算が高

速に実行可能であり、通常用いる標準型橙円曲線よりも高速にスカラー倍計算が実行可能である。

【0078】

標数2の有限体上で定義された橙円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された橙円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【0079】

図25は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第6実施例を示す図である。図22、図23及び図24は、第6実施例のスカラー倍計算方法を示すフローチャートである。図22～図25を参照して、第6実施例を説明する。

【0080】

スカラー倍計算装置2501では、点及びスカラー値2507を入力し、以下の手順でスカラー倍2508を出力する。ステップ2201として、繰り返し判定部2506において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ2202として、2倍算演算部2504により、点Pの2倍点2Pを計算する。ステップ2203として、スカラー倍計算装置2501に入力された点Pとステップ2202で求めた点2Pを、点格納部2502に点の組(P, 2P)として格納する。

【0081】

ステップ2204として、繰り返し判定部2506により、変数Iとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ2213へ行く。一致しなければステップ2205へ行く。ステップ2205として、変数Iを1増加させる。ステップ2206として、ビット値判定部2505により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ2401へ行く。そのビットの値が1であればステップ2301へ行く。

## 【0082】

ステップ2301として、演算ランダム化部2509により、加算及び2倍算の計算順序をランダム化する。加算、2倍算の順序で計算を実行する場合はステップ2305へ行く。2倍算、加算の順序で計算を実行する場合はステップ2302へ行く。

## 【0083】

ステップ2302として、2倍算演算部2504により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ2303へ行く。ステップ2303として、加算演算部2503により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2304へ行く。

## 【0084】

ステップ2305として、加算演算部2503により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $mP$ と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2306へ行く。ステップ2306として、2倍算演算部2504により、点格納部2502に格納されている点の組( $mP, (m+1)P$ )から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ2304へ行く。

## 【0085】

ステップ2304として、ステップ2303乃至はステップ2305で求めた点 $(2m+1)P$ とステップ2302乃至はステップ2306で求めた点 $(2m+2)P$ を点格納部2502に点の組 $((2m+1)P, (2m+2)P)$ として、点の組( $mP, (m+1)P$ )の代わりに格納する。その後ステップ2204へ戻る。

## 【0086】

ステップ2401として、演算ランダム化部2509により、加算及び2倍算